

SOUTH CAROLINA COMMISSION ON DISABILITIES AND SPECIAL NEEDS

MINUTES

November 19, 2020

The South Carolina Commission on Disabilities and Special Needs met on Thursday, November 19, 2020, at 10:00 a.m. at the Department of Disabilities and Special Needs Central Office, 3440 Harden Street Extension, Columbia, South Carolina.

The following were in attendance:

COMMISSION

Present In-Person

Gary Lemel – Chairman

Barry Malphrus – Vice Chairman

Robin Blackwood – Secretary

Eddie Miller

David Thomas

Present via Skype:

Stephanie Rawlinson

DDSN Administrative Staff

Mary Poole, State Director; Pat Maley, Deputy Director; Chris Clark, CFO; Rufus Britt, Associate State Director, Operations; Susan Beck, Associate State Director, Policy; Kevin Yacobi, Director of Internal Audit; Kim McLeod, Legislative Liaison & Public Information Officer; Andrew Tharin, Director of Engineering and Planning; Ann Dalton, Director of Quality Management; Melissa Ritter, Director of Head and Spinal Cord Injury (HASCI) and Christie Linguard, Administrative Coordinator.

Notice of Meeting Statement

Chairman Lemel called the meeting to order and Secretary Blackwood read a statement of announcement about the meeting that was distributed to the appropriate media, interested persons, and posted at the Central Office and on the website in accordance with the Freedom of Information Act.

Adoption of the Agenda

On motion of Commissioner Blackwood, seconded by Commissioner Malphrus, the Commission unanimously adopted the November 19, 2020 Meeting Agenda. (Attachment A)

Invocation

Chairman Lemel gave the invocation.

Approval of the Minutes from the October 14, 2020 Special-Called and the October 15, 2020 Commission Meetings

Commissioner Miller made a motion to accept the October 14, 2020 Special-Called Meeting minutes as written and to accept the October 15, 2020 Commission Meeting minutes with the addition of “for approval” in the second to the last sentence in section B under 2021 Spending Plan/Capital Budget; the motion was seconded by Commissioner Malphrus and unanimously approved by the Commission. (Attachment B)

Commissioners’ Update

Commissioner Thomas spoke briefly about his visit to Greenwood Genetics Center earlier in the month with Pat Maley. Commissioner Malphrus mentioned a great book he just read, *Help! My Sibling Has a Disability* by Dave Deuel. He recommended that everyone read this book.

Public Input

The following individuals spoke during Public Input: Jason Tavenner, Gerald Bernard and Ralph Courtney.

Commission Committee Business

A. Finance and Audit Committee

Committee Chairman Blackwood stated the Committee met on November 2, 2020 and presented the following topics for review and approval by the Commission:

Capital Project Review/Approval – Coastal Electrical Grid

Discussion was held on the proposal to replace the current grid and Andrew Tharin was present to answer all questions. Commissioner Lemel noted that the Finance and Audit Committee has already approved the proposal to replace the existing grid at the Coastal Center and the motion to approve was brought out of the Committee. The members of the Commission unanimously approved the proposal as presented. (Attachment C)

Contract Amendments over \$200k

Commissioner Blackwood informed the Commission that the Finance and Audit Committee approved the first two amendments listed but the last amendment by CHS Group was added after the Committee met. Commissioner Blackwood made a motion to accept the amendments

presented, seconded by Commissioner Malphrus and unanimously approved. (Attachment D)

General Duties of the DDSN Internal Audit Division (275-05-DD)

Commissioner Blackwood reminded everyone that this item was brought to the Commission meeting last month. After meeting the required posting for public comment, the Finance and Audit Committee has approved this directive as presented. Chairman Lemel noted that the Commission accepts the motion and second coming out of the Finance and Audit Commission and asked if any member opposed the directive as presented; there were five (5) ayes and one (1) nay (Chairman Lemel); the directive was approved as presented. Chairman Lemel was against the \$1,000 sanction included in this revised directive. (Attachment E)

B. Policy Committee

Committee Chairman Malphrus deferred the presentation of the following policy directive revisions to Ms. Beck. These revisions were reviewed and discussed at the November 10, 2020 Policy Committee meeting. Copies were previously provided to the Commission:

567-04-DD: DDSN Approved Crisis Prevention Curricula List and Curriculum Approval – After a brief summarization by Susan Beck, Chairman Lemel presented this directive as a motion and second coming out of the Policy Committee. After discussion, Commissioner Thomas asked if the word “prohibits” could be used instead of “does not approve” on page two under “Policy”. Commissioner Malphrus made a motion to approve the recommended change; seconded by Commissioner Blackwood and unanimously approved by the Commission. Commissioner Malphrus then made a motion to approve the directive with the aforementioned change; seconded by Commissioner Blackwood; and unanimously approved by the Commission. (Attachment F)

604-04-DD: Standard First Aid with Cardiopulmonary Resuscitation (CPR) - Adult, Child, Infant

This directive was referred from the Policy Committee for staff delegation and was posted for external review. A motion was made by Commissioner Malphrus to approve the directive as submitted, seconded by Commissioner Thomas; and unanimously approved by the Commission. (Attachment G)

367-02-DD: Acquiring Information Technology (IT) Products and Services

This directive was referred from the Policy Committee for staff delegation and was posted for external review. A motion was made by Commissioner Malphrus to approve the directive as submitted, seconded by Commissioner Rawlinson; and unanimously approved by the Commission. (Attachment H)

367-32-DD: Information Security and Privacy

This directive which combines 13 other directives, was written by the agency's Information Security division with the assistance of the Information Technology division. It was referred from the Policy Committee for staff delegation and was posted for external review. A motion was made by Commissioner Malphrus to approve the directive as submitted, seconded by Commissioner Blackwood; and unanimously approved by the Commission. (Attachment I)

100-11-DD: Absence with Leave of District Director or Facility Administrator from Duty Station

Ms. Beck asked that this directive be marked obsolete. Commissioner Rawlinson made a motion to mark this directive obsolete; seconded by Commissioner Malphrus and unanimously approved by the Commission. (Attachment J)

367-09-DD: Acceptable use of Network Services and the Internet; 367-12-DD: Service Provider Data Protection; 367-18-DD: Information Security Policy - Access Control; 367-19-DD: Physical Access and Environmental Security Policy; 367-21-DD: Data Protection and Privacy Policy; 367-22-DD: Information Security Policy - Asset Management; 367-23-DD: Information Security Policy Information Systems - Acquisitions, Development, and Maintenance; 367-24-DD: Information Security Policy - IT Compliance; 367-25-DD: Information Security Policy - IT Risk Strategy; 367-26-DD: Information Security Policy - Risk Management 367-27-DD: Information Security Policy - Threat and Vulnerability Management; 367-28-DD: Information Security Policy - Business Continuity Management; and 367-29-DD: Information Security Program Master Policy

The above directives are presented to the Commission for approval to mark them obsolete. On a motion by Commissioner Blackwood, seconded by Commissioner Malphrus, the directives above have been approved to mark them all as obsolete.

Other Committee Updates – Ms. Beck reported that there have been 18 complete reviews and also marked 18 directives as obsolete, which means the Policy Committee is on pace to complete the goal of 45 directives per year. Ms. Beck thanked the Committee and Commission

for their attention and diligence. State Director Poole thanked the staff for all of their hard work. Commissioner Malphrus announced that the next Policy Committee meeting will take place on January 12, 2021 at 3:00 PM. (Attachment K)

Old Business

A. HHS Admin Contract Update

SCDHHS State Director Joshua D. Baker joined the Commission meeting via telephone to discuss in detail the 2014 Administrative Contract with SCDHHS, which ended June 30, 2020. Mr. Clark noted that the current Administrative Contract is in process and will be ready for execution soon. Commissioner Thomas moved that the 2014 Administrative Contract be approved as presented; seconded by Commissioner Miller and unanimously approved by the Commission.

B. Band B & I Switch to Fee for Service (FFS) Update

Mr. Clark commenced by stating that the baseline data from 2019 was used in the documents presented. He went on to explain that providers from the Coalition as well as the SC Human Services Providers Association were nominated by their peers to attend agency meetings to discuss the different Band Options. The provider network overwhelming supported Option 2. After detailed discussion, Commissioner Malphrus made a motion to approve Option 1 and seconded by Commissioner Thomas. Discussion ensued after the motion and before the vote of four (4) ayes (Commissioners Blackwood, Malphrus Rawlinson and Thomas) and two (2) nays (Commissioners Lemel and Miller). Option 1 was approved by the Commission. (Attachment L)

C. Cost Reports Update

Mr. Clark briefed the Commission on the status of the agency's Cost Reports dating back to 2013. The 2017 Cost Report was filed on November 4, 2020 and is awaiting approval from SCDHHS.

D. Legislative Update

Ms. McLeod announced that the Notice of Drafting documents for the agency's Regulations must be submitted to the Legislative Council by December 11, 2020 to publish in the State Register. The Notices of Drafting are valid for one calendar year. The 2021 session begins a new two-year cycle for regulations. If the proposed regulations are not approved this year, the agency still has another full session for the regulations to be approved. Commissioner Thomas and Ms. McLeod will work together on a meeting date for the Legislative Committee. The SC

House of Representatives will have an Organizational Session on December 1-2, 2020. Senator Brad Hutto has replaced Senator Nikki Setzler as the Senate Minority Leader.

E. Internal Audit Monthly Report

Mr. Yacobi presented the cost for an external assessment review (\$27,600) and the cost for a self-assessment with an external party to validate (\$14,800) per the Institute of Internal Auditors. He added that these estimates are only good for one year; and the next review year for the agency is 2022.

F. Abuse Neglect and Exploitation (ANE) Quarterly Report

Ms. Dalton gave the ANE report for community residential, day service and regional centers. There was no further discussion after her presentation. (Attachment M)

G. COVID Update

Mr. Britt briefed the Commission on COVID policies, updated positive result numbers, requests for individuals to spend Thanksgiving with family members outside of their residential facilities and hazard/hero pay for staff members.

New Business

A. Financial Update

Mr. Clark gave the financial update as of October 31, 2020. On a motion by Commissioner Thomas, seconded by Commissioner Miller, the Commission unanimously approved the financial update as presented. (Attachment N)

B. Hiring & Retention Bonus for LPNs/Nurses at Regional Centers

Mr. Britt expressed the critical need to hire and retain nurses, especially during COVID. The proposal outlined was explained in great detail. On a motion by Commissioner Rawlinson, seconded by Commissioner Miller, the Commission unanimously approved the hiring & retention bonus plan for LPNs/Nurses at Regional Centers. (Attachment O)

C. Head and Spinal Cord Injury (HASCI) Waiver Waiting List

Ms. Ritter presented the HASCI Waiver Waiting List for approval. She briefly went over the reason for requesting a waiting list. Commissioner Miller made a motion to approve the creation of a HASCI Waiver Waiting

List; and the motion was seconded by Commissioner Blackwood and unanimously approved by five (5) Commission members. Commissioner Rawlinson abstained from participation in this vote. (Attachment P)

State Director's Report

Director Poole provided a State Director's Report. Ms. Poole has requested that the Commission schedule a Workgroup meeting in January. Commissioner Lemel stated that he will communicate with each member to finalize a date. (Attachment Q)

Executive Session

At 1:50 p.m., Chairman Lemel requested a motion to begin Executive Session to discuss an employment matter regarding the Executive Director. On a motion by Commissioner Blackwood, seconded by Commissioner Malphrus and unanimously approved by the Commission.

Upon rising out of Executive Session at 2:18 p.m., Chairman Lemel announced that there was no motions made, no decisions were rendered and no votes taken.

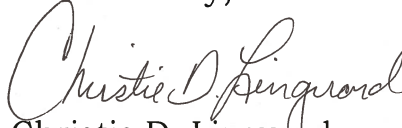
Next Regular Meeting

December 17, 2020

Adjournment

On a motion by Commissioner Blackwood, seconded by Commissioner Malphrus and unanimously approved by the Commission, the meeting was adjourned at 2:18 p.m.

Submitted by,


Christie D. Linguard

Approved:



Commissioner Robin Blackwood
Secretary

SOUTH CAROLINA COMMISSION ON DISABILITIES AND SPECIAL NEEDS**A G E N D A**

**South Carolina Department of Disabilities and Special Needs
3440 Harden Street Extension
Conference Room 251 (SKYPE)
Columbia, South Carolina**

November 19, 2020**10:00 A.M.**

1. Call to Order *Chairman Gary Lemel*
 2. Notice of Meeting Statement *Commissioner Robin Blackwood*
 3. Welcome
 4. Adoption of Agenda
 5. Invocation *Commissioner Gary Lemel*
 6. Approval of the October 14, 2020 Special-Called and October 15, 2020 Commission Meeting Minutes
 7. Commissioners' Update *Commissioners*
 8. Public Input
 9. Commission Committee Business
 - A. Finance and Audit Committee *Committee Chairman Robin Blackwood*
 1. Capital Project Review/Approval – Coastal Electrical Grid
 2. Contract Amendments over \$200,000
 3. General Duties of the DDSN Internal Audit Division (275-05-DD)
 - B. Policy Committee *Committee Chairman Barry Malphrus*
 - 567-04-DD: DDSN Approved Crisis Prevention Curricula List and Curriculum Approval
 - 604-04-DD: Standard First Aid with Cardiopulmonary Resuscitation (CPR) - Adult, Child, Infant
 - 367-02-DD: Acquiring Information Technology (IT) Products and Services
 - 367-32-DD: Information Security and Privacy
 - 100-11-DD: Absence with Leave of District Director or Facility Administrator from Duty Station (pg. 1-2)
 - 367-09-DD: Acceptable use of Network Services and the Internet (pg. 3-6)
 - 367-12-DD: Service Provider Data Protection (pg. 7-8)
 - 367-18-DD: Information Security Policy - Access Control (pg. 9-18)
 - 367-19-DD: Physical Access and Environmental Security Policy (pg. 19-22)
 - 367-21-DD: Data Protection and Privacy Policy (pg. 23-27)
 - 367-22-DD: Information Security Policy - Asset Management (pg. 28-29)
 - 367-23-DD: Information Security Policy Information Systems - Acquisitions, Development, and Maintenance (pg. 30-35)
 - 367-24-DD: Information Security Policy - IT Compliance (pg. 36-38)
 - 367-25-DD: Information Security Policy - IT Risk Strategy (pg. 39-41)
 - 367-26-DD: Information Security Policy - Risk Management (pg. 42-44)
 - 367-27-DD: Information Security Policy - Threat and Vulnerability Management (pg. 45-49)
 - 367-28-DD: Information Security Policy - Business Continuity Management (pg. 50-55)
 - 367-29-DD: Information Security Program Master Policy (pg. 56-61)
- Other Committee Updates

10. Old Business:

- | | |
|--|---|
| A. HHS Admin Contract Update | <i>DHHS Director Joshua Baker/Mr. Chris Clark</i> |
| B. Band B & I Switch to Fee for Service (FFS) Update | <i>Mr. Chris Clark</i> |
| C. Cost Reports Update | <i>Mr. Chris Clark</i> |
| D. Legislative Update | <i>Ms. Kim McLeod</i> |
| E. Internal Audit Monthly Report | <i>Mr. Kevin Yacobi</i> |
| F. ANE Quarterly Report | <i>Ms. Ann Dalton</i> |
| G. COVID Update | <i>Mr. Rufus Britt</i> |

11. New Business:

- | | |
|---|---------------------------|
| A. Financial Update | <i>Mr. Chris Clark</i> |
| B. Hiring & Retention Bonus for LPNs/Nurses at Regional Centers | <i>Mr. Rufus Britt</i> |
| C. HASCI Waiver Waiting List | <i>Ms. Melissa Ritter</i> |

- | | |
|--|----------------------------------|
| 12. State Director's Report | <i>State Director Mary Poole</i> |
| 13. Executive Session | |
| 14. Enter into Public Session | |
| 15. Next Regular Meeting (December 17, 2020) | |
| 16. Adjournment | |

SOUTH CAROLINA COMMISSION ON DISABILITIES AND SPECIAL NEEDS

SPECIAL-CALLED MEETING

MINUTES

October 14, 2020

The South Carolina Commission on Disabilities and Special Needs met on Wednesday, October 14, 2020, at 6:00 p.m. at the Embassy Suites Hotel (Salon G) at 200 Stoneridge Drive, Columbia, South Carolina.

The following were in attendance:

COMMISSION

Present In-Person:

Gary Lemel – Chairman
Barry Malphrus – Vice Chairman
Robin Blackwood – Secretary
Eddie Miller
Stephanie Rawlinson
David Thomas

DDSN Administrative Staff

Mary Poole, State Director

Call to Order

Chairman Lemel called the meeting to order and noted the purpose of this meeting will be to discuss a personnel matter.

Notice of Meeting Statement

Commissioner Blackwood read a statement of announcement about the meeting notice, which was distributed to appropriate media, interested persons, and posted at the Central Office and on the website in accordance with the Freedom of Information Act.

Adoption of the Agenda

On motion of Commissioner Miller, seconded by Commissioner Rawlinson, the Commission unanimously adopted the October 14, 2020 Special-Called Meeting Agenda. (Attachment A)

Executive Session

Chairman Lemel asked that the Commission entertain a motion to enter into Executive Session for purposes to discuss a personnel matter related to the

Executive Director. He also noted that, in Commissioner Thomas' motion at September's regularly scheduled Commission meeting, the record shows that the purpose of this special-called meeting is to discuss a personnel matter and that this has been a part of the record for almost a month now. On a motion by Commissioner Malphrus, seconded by Commissioner Miller, the Commission entered into Executive Session at 6:02 P.M.

Rise from Executive Session

At 8:03 P.M., the Commission rose out of Executive Session noting that there were no motions made, no votes taken and no decisions made. The issues discussed were strictly that of the Executive Director.

Adjournment

On motion of Commissioner Blackwood, seconded by Commissioner Miller and unanimously approved by the Commission, the meeting was adjourned at 8:04 P. M.

Submitted by,

Christie D. Linguard

Approved:

Commissioner Robin Blackwood
Secretary

SOUTH CAROLINA COMMISSION ON DISABILITIES AND SPECIAL NEEDS

MINUTES

October 15, 2020

The South Carolina Commission on Disabilities and Special Needs met on Thursday, October 15, 2020, at 10:00 a.m. at the Department of Disabilities and Special Needs Central Office, 3440 Harden Street Extension, Columbia, South Carolina.

The following were in attendance:

COMMISSION

Present In-Person

Gary Lemel – Chairman

Barry Malphrus – Vice Chairman

Robin Blackwood – Secretary

Eddie Miller

Stephanie Rawlinson

David Thomas

DDSN Administrative Staff

Mary Poole, State Director; Pat Maley, Deputy Director; Chris Clark, CFO; Rufus Britt, Associate State Director, Operations; Susan Beck, Associate State Director, Policy; Constance Holloway, General Counsel; Michael Mickey, Chief Information Officer; Kevin Yacobi, Director of Internal Audit; and Christie Linguard, Administrative Coordinator.

Notice of Meeting Statement

Chairman Lemel called the meeting to order and Secretary Blackwood read a statement of announcement about the meeting that was distributed to the appropriate media, interested persons, and posted at the Central Office and on the website in accordance with the Freedom of Information Act.

Adoption of the Agenda

On motion of Commissioner Rawlinson, seconded by Commissioner Malphrus, the Commission unanimously adopted the October 15, 2020 Meeting Agenda. (Attachment A)

Invocation

Commissioner Thomas gave the invocation.

Approval of the Minutes of the September 17, 2020 Commission Meetings

On motion of Commissioner Malphrus, seconded by Commissioner Thomas, the Commission unanimously approved the September 17, 2020 Commission Meeting minutes.

Commissioners' Update

Chairman Lemel announced that he attended MaxAbilities of York County's 40th (Ruby) Anniversary Celebration held on September 24, 2020 from 5:00 – 7:00 PM. A video highlighting the history of the center was shown.

Public Input

There were no requests for public input.

Commission Committee Business

A. Finance and Audit Committee

Committee Chairman Blackwood stated the Committee met on October 12, 2020 and presented the following topics for review and/or approval by the Commission:

Quarterly Provider Contracts Summary

Mr. Clark discussed the details on the contracts summary for those amounts over \$200,000. Amounts were approved in prior Commission meetings other than the one that being presented as the next topic. Commissioner Thomas made a motion to accept this summary as written, seconded by Commissioner Blackwood and approved unanimously by the Commission. (Attachment B)

Contract Amendments over \$200k

One contract amendment for Mentor exceeded the \$200,000 required approval amount. Chairman Lemel noted that the Finance and Audit Committee has already approved the contract amendments and the motion was brought out of the Committee. The members of the Commission unanimously approved the amendments presented. (Attachment C)

Internal Audit Committee Charter

Director of Internal Audits, Kevin Yacobi, presented the Internal Audit Committee Charter for the Commission's approval. Commissioner Malphrus made a motion to accept the Charter as edited by the Finance

and Audit Committee, seconded by Commissioner Thomas and unanimously approved by the Commission. (Attachment D)

Internal Audit Charter (275-05-DD)

Commissioner Rawlinson accepted this charter/directive as information only. After the ten (10) day public comment period, it will be taken back to the Finance and Audit Committee and then here to the Commission for final approval. (Attachment E)

B. Policy Committee

Committee Chairman Malphrus deferred the presentation of the following policy revisions to Ms. Beck. These revisions were reviewed and discussed at the October 13, 2020 Policy Committee meeting. Copies had previously been provided to the Commission:

603-12-DD: Immunization Procedure for DDSN Regional Centers – This updated policy now includes details from the Vaccination Information Policy (603-08-DD). Commissioner Rawlinson made a motion to approve this policy as presented, seconded by Commissioner Thomas and unanimously approved by the Commission. (Attachment F)

603-08-DD: Vaccination Information; 603-10-DD: Latex Protocol for DDSN Regional Centers; 300-06-DD: Energy Management Systems Operations and Parameters – Since each of the listed policies are addressed in other policies, Ms. Beck recommended that these policies be marked obsolete from the agency's directives. Commissioner Malphrus made a group motion to approve marking all three (3) policies as obsolete, seconded by Commissioner Rawlinson, and the unanimously approved by the Commission. (Attachment G)

Other Committee Updates – Commissioner Malphrus indicated that there are 14 directives associated with information security that will be combined and then sent out for public comment. He also thanked the Committee members for their hard work and noted that the Policy Committee will not meet in December.

Old Business

A. COVID Update

Mr. Britt briefed the Commission on COVID policies, updated positive result numbers and hazard/hero pay for staff members.

B. Office of the State Auditor Report-Corrective Action Plan

Mr. Clark shared the corrective action plan responses with the Commission. On a motion by Commissioner Miller, seconded by Commissioner Malphrus, the corrective action plan responses were unanimously approved by the Commission. (Attachment H)

C. Band B & I switch to Fee for Service (FFS) Update

Mr. Clark presented a chart/timeline and detailed discussion ensued about the Band B & I to FFS. This update was received as information only. (Attachment I)

D. Internal Audit Monthly Report

Mr. Yacobi provided the Commission members with standards for the professional practices of internal audits along with the latest self-assessment audit report completed for SFYs 2016 and 2017. These items were received as information only. (Attachment J)

E. Waiver Slots & Enrollment Process

Commission members were provided a copy of the May 2020 internal audit report analysis of the agency's waiver slots. Mr. Yacobi and Ms. Beck provided a brief overview of this analysis and answered questions from Commission members. (Attachment K)

New Business

A. Financial Update

Mr. Clark gave the financial update as of September 30, 2020. He reminded all Commission members that all state agencies are operating under a continuing resolution appropriation. On a motion by Commissioner Thomas, seconded by Commissioner Miller, the Commission unanimously approved the financial update as presented. (Attachment L)

B. 2021 Spending Plan/Capital Budget

Mr. Clark presented the 2021 Spending Plan and the Capital Budget/Expenditures. He noted high level assumptions and other components of the spending plan development. He called attention to the improvements made to the budget process including prior year comparatives with explanations. He expressed that the spending plan would be revised once the final State budget is approved unless we remain under a continuing resolution. Commissioner Thomas made a motion to approve the 2021 Spending Plan as presented, seconded by Commissioner Rawlinson, and unanimously approved by the

Commission members. A discussion was held regarding the current assumption that no financing of capital projects would be obtained, but that this is still a recommendation Mr. Clark stands by. Also, preliminary indications are that we will not need the full amount shown for vehicles to purchase the 30 vehicles recommended for replacement in 2021. Also, a discussion was held related to the need to renovate/improve the two electrical grids at two of the regional centers. Commissioner Miller made a motion to approve the Capital Budget/Expenditures as a whole but not the individual line items, which will come back to the Commission prior to spending the money. This motion was seconded by Commissioner Rawlinson and unanimously approved by the Commission members. (Attachment M)

C. VDI Computer Project Approval

Mr. Clark welcomed the new Chief Information Officer, Michael Mickey, who presented the VDI computer project software for purchase. On a motion by Commissioner Thomas, seconded by Commissioner Miller, the Commission unanimously approved the purchase of the new VDI software. (Attachment N)

D. HHS Admin Contract Update

Mr. Clark briefly gave background information on the Admin. Contract from HHS and answered any questions. This item was received as information only.

E. Appendix K Update

Mr. Clark gave a brief overview of Appendix K and informed the members of the Commission that he will continue to update them on an as needed.

F. State Director Review

Chairman Lemel asked each Commission member to complete their assessment forms for State Director Mary Poole and hand them to him after this meeting. He will compile and send to the SC Agency Head Salary Commission with a copy to Commission members for their record. On a motion by Commissioner Rawlinson, seconded by Commissioner Blackwood, the Commission unanimously approved the State Director's Review and the process by which it will be submitted.

State Director's Report

Director Poole provided a State Director's Report. (Attachment O)

Executive Session

At 1:32 p.m., Chairman Lemel requested a motion to begin Executive Session after a five minute break to discuss a personnel matter. On a motion by Commissioner Miller, seconded by Commissioner Rawlinson and unanimously approved by the Commission, executive session will began at 1:37 p.m.

Upon rising out of Executive Session at 2:04 p.m., Chairman Lemel announced that there was no action taken, no votes held and no motions made.

Next Regular Meeting

November 19, 2020

Adjournment

On a motion by Commissioner Thomas, seconded by Commissioner Malphrus and unanimously approved by the Commission, the meeting was adjourned at 2:05 p.m.

Submitted by,

Christie D. Linguard

Approved:

Commissioner Robin Blackwood
Secretary



Land Engineering Associates, LLC

262 Sandhurst Road, Suite 101
Columbia, SC 29210

phone: (803) 528-1437
email: Joe.Land.LEA@sc.rr.com

Andrew Tharin
SC Dept. of Disabilities & Special Needs (DDSN)
3440 Harden Street Extension
Columbia, SC 29203

October 29, 2020

RE: Proposal for Engineering Services – Coastal Center Electrical Power Grid Conversion – Phase 1

Dear Mr. Tharin,

The following is a fee proposal from Land Engineering Associates to provide Phase 1 electrical engineering services associated with the replacement of an existing 12.47 kV underground medium voltage power grid at DDSN's Coastal Center facility with a new 23.9 kV power grid.

Phase 1 – Schematic Design: Phase 1 services will be provided to inventory the existing electrical power grid infrastructure and develop a preliminary opinion of probable construction costs for the remaining new/replacement power grid infrastructure that is noted as not being included in Dominion Energy's proposal to DDSN dated May 29, 2019. A report will also be provided to describe the existing and new power grid infrastructure systems.

Phase 1 Lump Sum Fee Proposal: \$8,600.00

Phase 1 Reimbursable Expenses: We do not foresee any reimbursable expenses for Phase 1 services.

We appreciate the opportunity to work with the SC Department of Disabilities & Special Needs on this project. If you have any questions or comments, please contact me at the phone number or email address listed above.

Thank you for the opportunity to provide you with this proposal.

Sincerely,

A handwritten signature in black ink that reads "Joseph W. Land". The signature is written in a cursive, slightly slanted style.

Joseph W. Land, PE



Land Engineering Associates, LLC

262 Sandhurst Road, Suite 101
Columbia, SC 29210

phone: (803) 528-1437
email: Joe.Land.LEA@sc.rr.com

Andrew Tharin
SC Dept. of Disabilities & Special Needs (DDSN)
3440 Harden Street Extension
Columbia, SC 29203

October 29, 2020

RE: **Proposal for Engineering Services – Coastal Center Electrical Power Grid Conversion – Phase 2**

Dear Mr. Tharin,

The following is a fee proposal from Land Engineering Associates to provide Phase 2 electrical engineering services associated with the replacement of an existing 12.47 kV underground medium voltage power grid at DDSN's Coastal Center facility with a new 23.9 kV power grid.

Phase 2 – Construction Documents: Construction bid documents will be developed for the following:

- Adding new aboveground and underground raceways for 23.9 kV primary distribution infrastructure to support new transformers furnished by Dominion Energy. Raceway provisions will be designed in accordance with Dominion Energy's construction standards.
- Identifying new pad-mounted service transformer installation locations. This will be coordinated with both DDSN and Dominion Energy.
- Specifying a new concrete pad for each new pad-mounted service transformer in accordance with Dominion Energy's construction standards.
- If necessary, specify fencing to enclose new pad-mounted service transformers.
- Specifying new primary and secondary grounding infrastructure at each new pad-mounted service transformer.
- Specifying requirements for underground secondary service laterals (properly sized raceways and conductors) and associated splice/junction boxes necessary to tie new transformers into the existing service laterals for each building.
- Specifying requirements for the removal and disposal of all existing service transformers and all existing power grid infrastructure.
- Identifying and specifying requirements to tie existing street lighting into Dominion Energy's power grid.
- Determine a proposed schedule of electrical outages required to cut-over new transformers to each existing building.

Attendance for the following meetings will be provided:

- Pre-Bid Conference.
- Bid Opening.
- Pre-Construction Conference.

- Construction progress meetings.

The following contract administration services will be provided:

- Review and approval of submitted substitutions.
- Review of submittals and shop drawings.
- Provide inspections and provide a punchlist at final inspection.

Phase 2 Lump Sum Fee Proposal: \$57,200.00

Phase 2 Reimbursable Expenses: We do not foresee any reimbursable expenses for Phase 2 services.

We appreciate the opportunity to work with the SC Department of Disabilities & Special Needs on this project. If you have any questions or comments, please contact me at the phone number or email address listed above.

Thank you for the opportunity to provide you with this proposal.

Sincerely,

Joseph W. Land

Joseph W. Land, PE



FOR DEPARTMENT USE ONLY

CHE _____
 JBRC _____
 SFAA _____
 JBRC Staff _____
 ADMIN Staff _____
 A-1 Form Mailed _____
 SPIRS Date _____
 Summary _____

(For Department Use Only)

SUMMARY NUMBER

FORM NUMBER

PERMANENT IMPROVEMENT PROJECT REQUEST

1. AGENCY Code J16 Name South Carolina Department of Disabilities and Special Needs
 Contact Person Shirley A. Wilson Phone (803) 898-9801

2. PROJECT Project # _____ Name Coastal Center- Electrical Power Grid Conversion
 Facility # _____ Facility Name Coastal Center Campus Wide

County Code	18 - Dorchester <input type="checkbox"/>
New/Revised Budget	\$22,500.00

Project Type	4 - Replace Existing Facilities/Systems <input type="checkbox"/>
Facility Type	10 - Campus Wide <input type="checkbox"/>

3. CPIP PROJECT APPROVAL FOR CURRENT FISCAL YEAR
 CPIP priority number 2 of 9 for FY 22/23

4. PROJECT ACTION PROPOSED (Indicate all requested actions by checking the appropriate boxes.)

Establish Project	<input checked="" type="checkbox"/>	Decrease Budget	<input type="checkbox"/>	Close Project	<input type="checkbox"/>
Establish Project - CPIP	<input type="checkbox"/>	Change Source of Funds	<input type="checkbox"/>	Change Project Name	<input type="checkbox"/>
Increase Budget	<input type="checkbox"/>	Revise Scope	<input type="checkbox"/>	Cancel Project	<input type="checkbox"/>

5. PROJECT DESCRIPTION AND JUSTIFICATION
 (Explain and justify the project or revision, including what it is, why it is needed, and any alternatives considered. Attach supporting documentation/maps to fully convey the need for the request.)

DESCRIPTION: This request is for Phase I funding for high voltage electrical power distribution grid conversion at Coastal Center. The system is in need of major upgrade to avert catastrophic failure and turn over ownership to Dominion Energy. Dominion Energy will rebuild overhead facilities and replace the underground primary and all three phase transformers feeding the facility.

JUSTIFICATION: SCDDSN currently owns the Coastal Center electrical power distribution grid, but has no staff with this expertise to maintain the system. The overhead facilities and underground cable are far beyond their useful life and must be converted to Dominion Energy for safety and reliability reasons. Partial failures have occurred due to storms; therefore, SCDDSN wants to convert ownership to Dominion Energy and be proactive in ensuring the health and safety of our consumers.
 The cost of this project is estimated to be \$1,500,000.00

6. OPERATING COSTS IMPLICATIONS
 Attach Form A-49 if any additional operating costs or savings will result from this request. This includes costs to be absorbed with current funding.

7. ESTIMATED PROJECT SCHEDULE AND EXPENDITURES
 Estimated Start Date: December 2020 Estimated Completion Date: December 2022
 Estimated Expenditures: Thru Current FY: \$22,500.00 After Current FY: _____

8. ESTIMATES OF NEW/REVISED PROJECT COSTS

PROJECT #	
------------------	--

- 1. _____ Land Purchase ---->
- 2. _____ Building Purchase ---->
- 3. 22,500.00 Professional Services Fees
- 4. _____ Equipment and/or Materials ---->
- 5. _____ Site Development
- 6. _____ New Construction ---->
- 7. _____ Renovations - Building Interior ---->
- 8. _____ Renovations - Utilities
- 9. _____ Roofing - _____ Roof Age
- 10. _____ Renovations - Building Exterior
- 11. _____ Other Permanent Improvements
- 12. _____ Landscaping
- 13. _____ Builders Risk Insurance
- 14. _____ Other Capital Outlay
- 15. _____ Labor Costs
- 16. _____ Bond Issue Costs
- 17. _____ Other: _____
- 18. _____ Contingency

Land: _____ Acres
 Floor Space: _____ Gross Square Feet
 Information Technology _____
 Floor Space: _____ Gross Square Feet
 Floor Space: _____ Gross Square Feet

\$22,500.00 TOTAL PROJECT BUDGET

ENVIRONMENTAL HAZARDS	
Identify all types of significant environmental hazards (including asbestos, PCB's, etc.) present in the project and the financial impact they will have on the project.	
Type:	_____
<u>Cost Breakdown</u>	
Design Services	\$ _____
Monitoring	\$ _____
Abate/Remed	\$ _____
Total Costs	\$ <u>0.00</u>

9. PROPOSED SOURCE OF FUNDING

Source	Previously Approved Amount	Increase/Decrease	Original/Revised Budget	Transfer to/from Proj. #	Rev Object Code	Treasurer's ID Number	Rev Sub Fund	Exp Sub Fund
(0) CIB, Group			0.00 0.00		8115		3043	3043
(1) Dept. CIB, Group			0.00 0.00		8115		3143	3143
(2) Institution Bonds			0.00 0.00					3235
(3) Revenue Bonds			0.00 0.00					3393
(4) Excess Debt Service		22,500.00	22,500.00 0.00		4516	48800100	4660	3497
(5) Capital Reserve Fund			0.00 0.00		8895		3603	3603
(6) Appropriated State			0.00 0.00		8895	68800100	1001	3600
(7) Federal			0.00 0.00			78800100		5787
(8) Athletic			0.00 0.00			88800100		3807
(9) Other (Specify)			0.00 0.00 0.00			98800100		3907
TOTAL BUDGET	\$0.00	\$22,500.00	\$22,500.00					

10. SUBMITTED BY: Chris Clark, Chief Financial Officer
 Signature of Authorized Official and Title

11/14/20
 Date

11. APPROVED BY: _____
 (For Department Use Only) Authorized Signature and Title

 Date

**ADDITIONAL ANNUAL OPERATING COSTS / SAVINGS
RESULTING FROM PERMANENT IMPROVEMENT PROJECT**

1. AGENCY Code J16 Name South Carolina Department of Disabilities and Special Needs

2. PROJECT Project # Name Coastal Center - Electric Power Grid Conversion

3. ADDITIONAL ANNUAL OPERATING COSTS / SAVINGS. (Check whether reporting costs or savings.)

COSTS SAVINGS NO CHANGE

4.

TOTAL ADDITIONAL OPERATING COSTS / SAVINGS					
Projected Financing Sources					
	(1)	(2)	(3)	(4)	(5)
	Fiscal Year	General Funds	Federal	Other	Total
1)	2020-21	\$	\$	\$	\$ 0.00
2)	2021-22	\$	\$	\$	\$ 0.00
3)	2022-23	\$	\$	\$	\$ 0.00


5. If "Other" sources are reported in Column 4 above, itemize and specify what the other sources are (revenues, fees, etc.).
N/A

6. Will the additional costs be absorbed into your existing budget? YES NO
If no, how will additional funds be provided?

7. Itemize below the cost factors that contribute to the total costs or savings reported above in Column 5 for the first fiscal year.

	<u>COST FACTORS</u>	<u>AMOUNT</u>
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____
5.	_____	_____
6.	_____	_____
7.	_____	_____
8.	_____	_____
	TOTAL	S0.00

8. If personal services costs or savings are reported in 7 above, please indicate the number of additional positions required or positions saved.

9. Submitted By:  Chris Clark, Chief Financial Officer
Signature of Authorized Official and Title

11/4/20
Date

Permanent Improvement Project Budget Load Worksheet

Basic Project Information

Agency Number J160 SPIRS Number 99XX
Project Name Coastal Center - Electrical Power Grid Conversion

For Existing Projects Only

State Funded Program
WBS Number

Project Systems Project Information

Project Type M-Mixed
Cost Center J160AE0010
Functional Area J160_2400

In general, projects will be created with only a Level 1 WBS. If you would like an existing project to be copied, you can request that. If you have other special requests please include those here. If you do request that a project be copied, it is your responsibility to check to make sure that all changes have been made appropriately before the project is released. Other requests will be considered if appropriate and resources allow.

Special Requests

Copy from Project WBS: M.J160.0087 Project: 9890

Other Requests (Explain)

Budget Load Information

In general, budgets will be loaded at the high level fund. If you would like the budget loaded at the 8 digit fund, please indicate that here. Please note that, as of now, EBO cannot load bond funds at the 8 digit fund.

Funding Source 1		Funding Source 2	
8 Digit Fund	34978000	8 Digit Fund	
Fund Center	J160AE00	Fund Center	
Functional Area	J160_2400	Functional Area	
Amount	22,500	Amount	
Action	Increase	Action	

Funding Source 3		Funding Source 4	
8 Digit Fund		8 Digit Fund	
Fund Center		Fund Center	
Functional Area		Functional Area	
Amount		Amount	
Action		Action	

For EBO Use Only

State Funded Program
WBS Number
Document Number(s)
Analyst

SECTION 1: GENERAL – TO BE PROVIDED FOR ALL PROPOSALS

1. Provide the internal projected cost of the project.

The projected cost of the project is \$1,500,000.

2. Identify the sources of funds to be used for A&E pre-design.

The source of funds to be used for A&E pre-design is excess debt service funds invested and held by the State Treasurer's Office on behalf of SCDDSN.

3. Describe and define each fund source to be used for A&E pre-design, with specificity. Cite any statutory authority, including the code section or other provision of law for use of the funds for permanent improvement projects. If the source includes any fee, provide the name of the fee, the fee amount, the frequency of collection and when the fee was first implemented.

SCDDSN's definition of the source of funds to be used for the A&E pre-design is excess debt service funds accumulated, deposited, and applied to capital improvements pursuant to SC Code of Laws §44-20-1160 and §44-20-1170.

§44-20-1160

Upon receiving the approval of the State Fiscal Accountability Authority the commission shall obligate itself to apply all monies derived from its revenues to the payment of the principal and interest of its outstanding obligations and those to be issued and to deliver to the board its obligations.

§44-20-1170

Following the execution and delivery of its obligations, the commission shall remit to the State Treasurer all its revenues, including accumulated revenues not applicable to prior obligations, for credit to a special fund. The special fund must be applied to meet the sums due by the commission under its obligations. These monies from the special fund must be applied by the State Treasurer to the payment of the principal of and interest on outstanding state capital improvement bonds.

If the accumulation of revenues of the commission in the special fund exceeds the payment due or to become due during the then current fiscal year and an additional sum equal to the maximum annual debt service requirement of the obligations for a succeeding fiscal year, the State Fiscal Accountability Authority may permit the commission to withdraw the excess and apply it to improvements that have received the approval of the board or to transfer the excess out of the special fund for contract awards to local disabilities and special needs boards for needed improvements at the local level and for nonrecurring prevention, assistive technology, and quality initiatives at the regional centers and local boards.

4. Provide the current uncommitted balance of funds for each source described above.

The current fund balance of uncommitted funds is \$2,286,837.89 – Please see attached spreadsheet.

5. Identify the sources of funds for construction.

The source of funds to be used for construction is excess debt service funds invested and held by the State Treasurer's Office on behalf of SCDDSN.

6. Describe and define each fund source to be used for construction, with specificity. Cite any statutory authority, including the code section or other provision of law for use of the funds for permanent improvement projects. If the source includes any fee, provide the name of the fee, the fee amount, the frequency of collection and when the fee was first implemented.

SCDDSN's definition of the source of funds to be used for construction is excess debt service funds accumulated, deposited, and applied to capital improvements pursuant to SC Code of Laws §44-20-1160 and §44-20-1170, as delineated above for question 3.

7. Provide the current uncommitted balance of funds for each source described above.

The current fund balance of uncommitted funds is \$2,286,837.89 --Please see attached spreadsheet.

8. Provide the total square footage of the building to be renovated or constructed.

The project's square footage encompasses the entire campus wide electrical power grid system, which sits on 142.66 acres, 6,214,269.6 Sq. Ft.

9. If any portion of the building is to be renovated, provide the square footage of the portion that will be included in the renovation.

The project encompasses Coastal Center's entire campus.

10. Describe the programs that will use the constructed or renovated space.

None.

11. Provide the current age of the building and building systems to be renovated or replaced.

This project encompasses the entire campus wide electrical power distribution system. The existing system was installed 1966 and is 54 years old. Transformers have failed recently. More failures are anticipated, as the system is well beyond life expectancy.

12. If any new space is being added to the facility, provide demand and usage data to support the need.

No new space is being added to the facility.

13. If the A&E pre-design request exceeds 1.5% of the internal estimated cost of the project, provide the reason the amount exceeds 1.5%.

A&E pre-design will not exceed 1.5% of the internal estimated cost of the project.

14. Provide an estimate of the numbers of students, faculty, staff and clients that are expected to utilize the space associated with the project or building.

The estimated number expected to utilize Coastal Center campus is 142 residents plus staff of 313.

15. Indicate whether or not the project has been included in a previous year's CPIP. If so, provide the last year the project was included and year for which it was proposed.

The project has not been included in a previous year's CPIP.

16. Provide the economic impact of the project or project request, including job creation and retention. If there is no economic impact, provide an explanation.

See attached economic impact projection.

17. Discuss how maintenance of this facility construction/renovation will be addressed and funded.

No increased or additional maintenance budget or staff will be required as a result of this electrical power grid conversion.

18. Provide the name of any account from which costs of deferred maintenance are addressed and its current uncommitted balance. Indicate the sources used to fund the account.

The agency has a deferred maintenance account, Non-PIP, expended \$99,661. which currently has an uncommitted balance of \$275,339. These funds are set aside under funding source 31490000.

19. If funding for maintenance of this facility construction/renovation has not yet been determined, discuss the steps that have been taken to address and fund maintenance of this and other facilities owned or managed by the agency or institution.

N/A

SECTION 2 – TO BE PROVIDED FOR HIGHER EDUCATION PROPOSALS

20. Indicate whether or not the use of any funds for construction will require an increase in any student fee or tuition. Describe any increase in student fees effected in prior years that has contributed to the availability of these funds.

21. If the use of any funds for construction includes any student fee, provide the name of the fee, the fee amount, the frequency of collection and when the fee was first implemented.

22. Provide a five-year history of each component within the institution's tuition and fee structure designated or utilized for permanent improvements. Identify the tuition or fee component per student, per semester; the total revenue collected during the academic year; and the fund balance at fiscal year end, all delineated by academic year. Include a projection for the ensuing academic year, and any future academic years in which the fee is projected to increase. Use the following format in responding to this question and provide as many tables as are necessary to promote a clear understanding of the relationship of tuition and fee revenue designated by the institution for permanent improvements, maintenance and other facility-related expense, including debt service.

Academic Year	Amount per student per semester	Total Revenue Collected During Academic Year	Amount Expended for Permanent Improvements	Fund Balance at Year End
2014-15				
2015-16				
2016-17				
2017-18				
2018-19				
2019-20*				

*Projection

23. Identify any other funds not specifically designated that may be utilized or redirected for permanent improvements, maintenance and other facility-related expense, including debt service. Provide a five-year history of total collections, by fund; amounts applied to or for permanent improvements, maintenance and other facility-related expense, including debt service; and the fund balance at fiscal year end, delineated by academic year. Include a projection for the ensuing academic year, and any future academic years in which the revenue is projected to increase. Describe any portion of the source that originates from any tuition or fee component. Include all permanent improvements without regard to Joint Bond Review Committee or State Fiscal Accountability approval requirements. Use the following format in responding to this question and provide as many tables as are necessary to provide a complete and comprehensive response for each fund.

Fund Source or Name:

Description:

Academic Year	Total Revenue Collected During Academic Year	Portion Collected From Tuition or Fee Revenues	Amount Expended for Permanent Improvements	Fund Balance at Year End
2014-15				
2015-16				
2016-17				
2017-18				
2018-19				
2019-20*				

*Projection

24. Describe the fund sources reflected above that will be utilized to support the project that is the subject of this Phase I proposal.

SC Department of Disabilities and Special Needs
 FYE 06/30/2021 - Report of Debt Service Account Activity
 Pursuant to Proviso

Beginning Balance for E-16 4660 as of 06/30/2020

\$2,276,184.17

Uses:

Total Uses

\$0.00

Sources:

Other Deposits

Interest Jul-20
 Interest Aug-20
 Interest Sep-20
 Interest Oct-20
 Interest Nov-20
 Interest Dec-20
 Interest Jan-21
 Interest Feb-21
 Interest Mar-21
 Interest Apr-21
 Interest May-21
 Interest Jun-21

\$3,092.02
 \$4,754.88
 \$2,806.82

Total Sources

\$10,653.72

Refunds from Closed Projects as of 09/30/2020

Total Sources

\$0.00

Balance Per STO Report for E-16 4660 as of 9/30/2020

\$2,286,837.89

DDSN Commission Approved Projects sent to JBRC/EBO as of 9/30/2020

Approved :

CPIP 19-20	Project	9926	Phase 1	Regional Centers R22 Refrigerate	(\$7,500.00)
CPIP 19-20	Project	9927	Phase 1	Replacement of Generator and Transfer Switches - CC - Dorm 110 & 210	(\$2,250.00)
CPIP 19-20	Project	9927	Phase 2	Replacement of Generator and Transfer Switches - CC - Dorm 110 & 210	(\$167,750.00)
CPIP 19-20	Project	9928	Phase 1	Replacement of VAV Terminals and EM Controls - WC - Dorm 205	(\$4,125.00)

Pending Approval :

Total

(\$181,625.00)

DDSN Commission Approved Projects as of 9/30/2020 - DDSN Preparing Submission to SC Department of Administration or State Fiscal Accountability Authority:

CPIP 19-20	Project	9928	Phase 2	Replacement of VAV Terminals and EM Controls - WC - Dorm 205	(\$270,875.00)
CPIP 19-20	Project	9926	Phase 2	Regional Centers R22 Refrigerate	(\$542,500.00)

Sub-total

(\$813,375.00)

Unobligated E-16 4660 as of 9/30/2020

\$1,291,837.89

*** SCDDSN owns approximately 200 buildings statewide which have a historical cost in excess of \$100 Million when combined with Building Improvements and Land Improvements. The above unobligated amount is 2% of that value and is available for timely response to emergencies, necessary repairs and disasters to ensure the safety of consumers and Federal / State compliance.

E. Mason 9/10/2020

Preparer and Date

Reviewer and Date

SCDDSN - COASTAL CENTER - ELECTRICAL POWER GRID CONVERSION

PHASE I (SCHEMATIC DESIGN FUNDING) ECONOMIC IMPACT

AGC of America Economic Impact Data	Projected Economic Impact of Proposed Project
99xx	
\$1,000,000,000	\$22,500 Phase I A&E Services investment
\$3,400,000,000	\$76,500 total increase to Gross Domestic Product
\$1,100,000,000	\$24,750 total increase in personal earnings
28500	0.6 total jobs created or sustained
9700	0.2 total on-site construction jobs created
4600	0.1 total indirect materials/service jobs created
14300	0.3 total jobs induced when construction & supplier workers spend income

PHASE II (FULL FUNDING) ECONOMIC IMPACT

AGC of America Economic Impact Data	Projected Economic Impact of Proposed Project SW-Reg. Ctrs.-Web-Based Energy Mgmt. Controls System Replacement
99xx	
\$1,000,000,000	\$1,500,000 total construction investment
\$3,400,000,000	\$5,100,000 total increase to Gross Domestic Product
\$1,100,000,000	\$1,650,000 total increase in personal earnings
28500	42.8 total jobs created or sustained
9700	14.6 total on-site construction jobs created
4600	6.9 total indirect materials/service jobs created
14300	21.5 total jobs induced when construction & supplier workers spend income

The Economic Impact of Construction in the United States and South Carolina

Economic Impact of Construction:

- U.S. gross domestic product (GDP)—the value of all goods and services produced in the country—totaled \$21.4 trillion in 2019; construction contributed \$887 billion (4.1%).
- In South Carolina, construction contributed \$12.6 billion (5.1%) of the state's GDP of \$246.3 billion.
- There were 706,000 construction firms in the U.S. in 2017, including 9,690 in South Carolina.

Construction Spending:

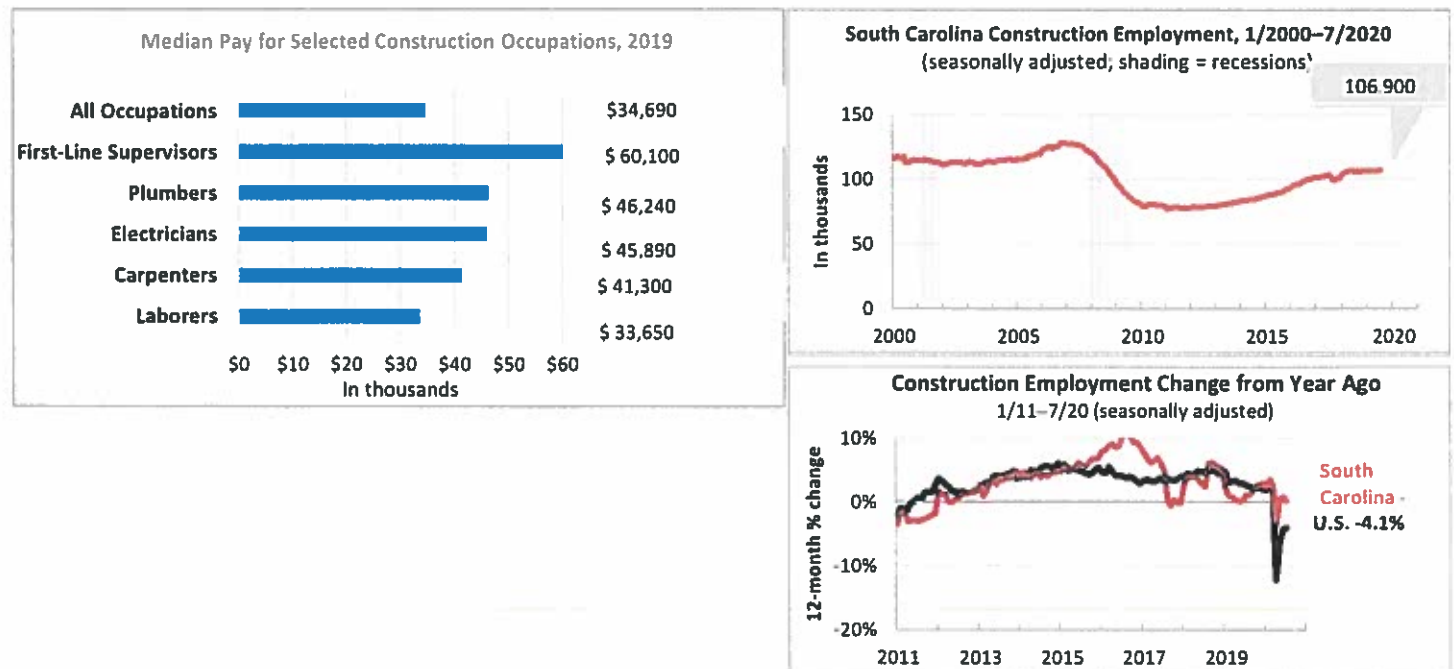
- Nonresidential spending in the U.S. totaled \$814 billion in 2019 (\$486 billion private, \$328 billion public).
- Residential construction spending in the U.S. totaled \$551 billion (\$280 billion single-family, \$80 billion multifamily, \$184 billion improvements, \$6 billion public).
- Private nonresidential spending in South Carolina totaled \$5.5 billion in 2019. State and local spending totaled \$4.5 billion. (Totals are not available for residential or federal construction spending).

Construction Employment (Seasonally Adjusted):

- Construction (residential + nonresidential) employed 7.2 million workers in July 2020, a decrease of 306,000 (-4.1%) from July 2019, and 6.6% less than in April 2006, when U.S. construction employment peaked.
- Construction employment in South Carolina in July 2020 totaled 106,900, a decrease of 0.1% from July 2019, and 16% less than the state's peak in October 2006.
- Contractors are hiring. In the 2020 AGC-Autodesk Workforce Survey, 60% of firms in the U.S. had unfilled hourly craft positions on June 30, 2020.

Construction Industry Pay:

- Construction jobs pay well. In South Carolina, 4 out of the 5 most numerous construction occupations had higher median pay than the median for all employees in the state in 2019. (Half of workers earn more than the median; half earn less.)



2021 Residential Amendments for Review

	Amendment #2	FY 2021	Description
Babcock Center	Capitated- CSW	\$ (15,045)	Decrease in one Band I
Babcock Center	Capitated- CTH I	\$ (34,250)	Termination of CTH I for WF
Babcock Center	Capitated- CTH II	\$ 48,138	Various CTH II moves, band changes
Babcock Center	Capitated- SLP II	\$ 67,009	Restoration of vacancies at Sandwood and Pitts Apts
Babcock Center	Capitated- ICF	\$ 204,413	Restoration of vacancies at Batesburg and Archie ICF
Babcock Center	Special HASCI Residential	\$ 75,727	Placement of HASCI Consumer- CJ at Gabriel House
Babcock Center	Less Bed Fees	\$ (5,947)	Related to ICF bed restorations
Babcock Center	Less Client Fees	\$ (15,236)	Related to ICF bed restorations
		\$ 324,809	
	Amendment #2	FY 2021	Description
Tri-Development Center	Special HASCI Residential	\$ 78,712	Placement of HASCI Consumer - CK at Lawson Rd
Tri-Development Center	Capitated- CTH I	\$ (39,143)	Termination of CTH I for PL
Tri-Development Center	Capitated- ICF	\$ (4,660)	Vacancy @ Linden until filled by ME
Tri-Development Center	Capitated- CTH II	\$ 15,797	Vacancy @ Trolley Line until filled by DT
Tri-Development Center	Capitated- CTH II	\$ 79,079	Restoration of vacancy @ Hillside for PL
Tri-Development Center	Capitated- CTH II	\$ 77,325	Restoration of vacancy @ Jewell for RW
Tri-Development Center	Refund of Bed Fees	\$ 136	Refund of Bed Fees related to vacancy
Tri-Development Center	Refund of Client Fees	\$ 249	Refund of Client Fees related to vacancy
		\$ 207,495	
	Amendment #1	FY 2021	Description
CHS Group	Residential Services	\$ 393,090	Services for 5 CTH II consumers
		\$ 393,090	

Mary Poole
State Director
Patrick Maley
Deputy Director
Rufus Britt
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
W. Chris Clark
Chief Financial Officer



3440 Harden Street Extension
 Columbia, South Carolina 29203
803/898-9600
Toll Free: 888/DSN-INFO
Home Page: www.ddsn.sc.gov

COMMISSION
Gary C. Lemel
Chairman
Barry D. Malphrus
Vice Chairman
Robin B. Blackwood
Secretary
Eddie L. Miller
Stephanie M. Rawlinson
David L. Thomas

Reference Number: 275-05-DD

Title of Document: General Duties of the South Carolina Department of Disabilities and Special Needs (DDSN) Internal Audit Division

Date of Issue: February 14, 2002

Effective Date: April 16, 2017

Last Review: November 19, 2020

Date of Last Revision: November 19, 2020 **(REVISED)**

Applicability: DDSN Central Office, DDSN Regional Centers and all providers of DDSN Sponsored Services including: Adult Companion Providers, Case Management Providers, Day Service Providers (i.e., career prep, day activity, community services, support center), Early Intervention Providers, Employment Services Providers, Financial Management Providers, HASCI Rehabilitation Support Providers, Intermediate Care Facilities for Individuals with Intellectual Disabilities (ICF/IID) Providers, Intake Providers, Residential Habilitation Providers and Respite Providers.

Purpose and Mission

The South Carolina Department of Disabilities and Special Needs (DDSN's) Internal Auditing (IA) is an independent, objective assurance and consulting activity designed to add value and improve the agency's/service providers' operations. It helps the organization accomplish their objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, governance, and the implementation of best practices.

Standards

IA will govern itself by adherence to the mandatory elements to The Institute of Internal Auditors International Professional Practices Framework, including the Core Principles for the

Professional Practice of Internal Auditing, the Code of Ethics, the *International Standards for the Professional Practice of Internal Auditing*, and the Definition of Internal Auditing.

Authority

It is the policy of DDSN to establish and support an Internal Audit Division as an independent appraisal function to examine and evaluate DDSN and provider activities as a service to Executive Management and the DDSN Commission.

The State Director shall appoint the Director of Internal Audit, subject to the approval of the full DDSN Commission. The Director of Internal Audit shall be responsible for the day-to-day administration and operation of the Internal Audit Division, subject to policies, rules and regulations adopted by the DDSN Commission.

Subject to the approval of the State Director, the Director of Internal Audit shall prescribe the organizational structure and the personnel necessary to carry out the Internal Audit function.

The Director of Internal Audit reports administratively to the State Director and functionally to the Finance/Audit Committee Chair of the DDSN Commission.

An annual audit plan will be developed by the Director of Internal Audit and submitted for review to the State Director, reviewed and approved by the Finance/Audit Committee, with final approval by the DDSN Commission. If adjustments are necessary due to changes in needs or priorities of DDSN, the changes will be coordinated with affected personnel.

In carrying out their responsibilities, members of the Internal Audit Division will have full, free, and unrestricted access to all DDSN funded service provider organizations' activities, records (manual and electronic), property, and personnel, and to the Finance/Audit Committee of the Commission, as necessary.

The Director of Internal Audit will have unrestricted access to, and communicate and interact directly with, the Audit Committee, including in private meetings without management present.

To establish, maintain, and assure that DDSN IA has sufficient authority to fulfill its duties, the Audit Committee will:

- Approve the IA Division's internal audit charter;
- Approve the Internal Audit Committee Charter;
- Approve the audit plan;
- Approve the internal audit budget and resource plan;
- Receive communications from the Director of Internal Audit on the internal audit division's performance relative to the plan and other matters;
- Approve decisions regarding the appointment and removal of the Director of Internal Audit;
- Approve the remuneration of the Director of Internal Audit; and
- Make appropriate inquiries of management and the Director of Internal Audit to determine whether there is inappropriate scope or resource limitations.

Independence and Objectivity

The DDSN Internal Audit Division is a staff function, and as such, does not have any responsibility or authority over areas that are being audited; therefore, any review or recommendation by Internal Audit will not in any way relieve the supervisor of the assigned responsibilities inherent with his/her position.

The Director of Internal Audit will ensure that the IA Division remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of audit selection, scope, procedures, frequency, timing, and report content. If the Director of Internal Audit determines that independence or objectivity may be impaired in fact or appearance, the details of the impairment will be disclosed to the appropriate parties.

Internal auditors will maintain an unbiased mental attitude that allows them to perform engagements objectively and in such a manner that they believe in their work product, that no quality compromises are made, and that they do not subordinate their judgment on audit matters to others.

Scope of IA Activities

The primary objective of the Internal Audit Division is to assist members of management in the effective discharge of their responsibilities by reviewing activities/programs and providing analyses, recommendations, and information regarding the activities/programs reviewed. The reviews are conducted to assure DDSN and its provider organizations comply with applicable State/Federal laws, standards, directives, policies, procedures and regulations. As such, the DDSN Internal Audit Division is concerned with all phases of DDSN and its provider organizations' operations. To this end, the Internal Audit Division will:

- 1) Determine the adequacy, efficiency, and effectiveness of systems of internal accounting and operating controls;
- 2) Determine the accomplishment of established goals and objectives;
- 3) Review and determine the reliability and integrity of financial information;
- 4) Determine the means of safeguarding assets and consumer funds;
- 5) Review and determine compliance with policies, procedures, laws, and regulations; and
- 6) Should Internal Audit discover a conflict of interest regarding any DDSN staff, the Audit Director will report such conflict to the Finance Audit Committee in Executive Session.

Activities

Specific internal audit responsibilities are as follows:

1. Perform scheduled audits of service provider organizations, DDSN Regional Centers, and DDSN Central Office for the effectiveness of operations and compliance with established standards and policies.
2. Perform special request audits in response to allegations/complaints/concerns of a financial or programmatic nature.
3. Provide consultation, technical assistance, and training to DDSN Divisions, DDSN Regional Centers and the service provider organizations.
4. Review, evaluate, and follow up on internal audit findings and recommendations with appropriate management staff.
5. Coordinate internal audit efforts with external auditors/reviewers.
6. Report to the DDSN Commission as requested to outline internal audit activities and review completed reports.

Audit Process/Steps

DDSN Internal audits will be conducted in accordance with this policy and with the procedures outlined in the DDSN *Audit Procedures Manual*. Generally, an audit of any activity or facility will consist of the following steps with the exception for a special audit (i.e., cash related, suspected fraud, etc.) which will be conducted on a no-notice or short notice basis.

1. When practical (i.e., time or type of audit), an engagement memo will be issued prior to a scheduled audit. The purpose of the engagement memo is to notify management of the area to be reviewed, describe the audit to be performed, and to request items needed at the onset of the review. If time does not permit, management will be notified by telephone and/or e-mail as soon as possible.
2. Preliminary planning consists of consideration being given to: any prior audit results (if applicable); internal controls; record keeping employed; documentary evidence required (i.e., required by policy, procedure, law, regulation, etc.); applicable policies and procedures; prior reviews by external and internal parties; and the type of report to be issued.
3. An audit program will be developed based on decisions reached during the preliminary planning. The program will be modified as dictated by discoveries made during the audit.
4. An entrance conference will be conducted between the auditor and management of the work unit(s) to be reviewed to discuss the nature of the audit, the areas to be audited, and the support required.

5. Fieldwork will consist of inquiry of appropriate personnel, observation of applicable activities, and examination of applicable records and documents. Fieldwork will depend on the type of audit being performed as well as the type of activity, operation, or program being reviewed.
6. The auditor will conduct an exit conference with management at the conclusion of the fieldwork to discuss the results of the audit. The exit conference should be a summary of concerns noted during the review that were communicated to auditee management throughout the engagement.
7. Findings will be documented after the completion of the fieldwork. These draft findings will be sent to the appropriate manager for the area being audited with a request that the findings be reviewed and corrective action plans be submitted to DDSN Internal Audit within 30 calendar days, or less, per DDSN Internal Audit's request.

Reporting

A draft report will be issued upon receipt of an acceptable corrective action plan; the draft will then be forwarded to the auditee for a final review for completeness and accuracy with follow-up to Internal Audit staff regarding any corrections/concerns detailed in the draft report.

Upon receiving the auditee's corrective action plan, Internal Audit staff will review actions to ensure satisfactory disposition of the audit findings and recommendations. If a corrective action plan is considered unsatisfactory, DDSN Internal Audit staff will hold further discussions to achieve acceptable disposition. If a mutually acceptable corrective action plan cannot be attained, an auditor's comment may be noted in the final report.

Once the draft report is accepted by both parties, a final report will be issued which incorporates the findings and submitted corrective action plans.

The results of formal audits and/or investigations will be reported to appropriate management based on the entity reviewed. In almost all cases (exceptions being criminal cases where DDSN Internal Audit staff is assisting law enforcement and is precluded from discussing the review based on the signing of non-disclosure statements), audit reports will be shared with the DDSN State Director, DDSN Commissioners, appropriate DDSN management levels, and in the case of provider organizations, the Executive Director and members of the organizations' governing board.

Financial Sanctions

A financial sanction, by way of a contract withhold, is only applicable to repeat findings as they relate to the health, safety and/or welfare of individuals being served.

The sanction will only apply when a follow-up audit is conducted and finds the accepted corrective action from the initial audit was not implemented. The Provider will then be given notice and be allowed 90 days to implement the agreed upon corrective action. If in the subsequent visit (i.e., the third visit), the corrective action plan was not implemented, the Provider will receive a financial sanction in the amount of a minimum of \$1,000 with a potential increase based on the discretion of the Finance Audit Committee.

An appeals process will be available to any Provider who is assessed a financial sanction. The appeal shall be requested within 30 days of notice of the sanction. The Appeals Committee membership will include: two (2) DDSN staff members; two (2) community provider members from each provider association; and one (1) consumer or family member. Once appointed, the Appeals Committee shall decide among the membership who shall be named as chair. Once appointed, the members shall serve for two (2) years.

Statement on Fraud

Auditors should be alert to situations (i.e., observations, informants) or transactions that could indicate actual or potential fraud or abuse, and consider extending audit steps and procedures, as necessary, to determine the effect of fraud on the audit results. The Audit Director should be made aware as soon as the auditor discovers potential or suspected fraud.

Auditors should exercise due professional care in pursuing indications of suspected fraudulent activity so as to avoid mistaken accusations or alerting suspected individuals and to not interfere with potential investigations or legal proceedings. If an auditor suspects fraud, embezzlement, or other possible criminal conduct, this should be discussed with the Auditor-In-Charge before proceeding further. The Auditor-In-Charge will in turn initiate a conference with the DDSN Audit Director and any other parties deemed appropriate (i.e., DDSN General Counsel). Depending on the extent and severity of the suspected fraud, appropriate reporting to the responsible entity (i.e., local law enforcement, SLED, etc.) will take place, and fieldwork in the area may be discontinued temporarily.

If the findings from an audit give the auditor reason to believe that fraud may have occurred in the Medicaid program, under the Code of Federal Regulations, [42 CFR §455.15](#), then the case must be referred to the Medicaid Fraud Control Unit (MFCU) in the South Carolina State Attorney General's Office.

Quality Assurance and Improvement Program

IA will maintain a quality assurance and improvement program that covers all aspects of the internal audit activity. The program will include an evaluation of the internal audit activity's conformance with the Definition of Internal Audit and the *Standards*, and an evaluation of whether the internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement.

The Director of Internal Audit will communicate to senior management and the Commission on the internal audit activity's quality assurance and improvement program, including results of ongoing internal assessments, and external assessments conducted at least every five years.

Barry D. Malphrus
Vice Chairman

Gary C. Lemel
Chairman

Mary Poole
State Director
Patrick Maley
Deputy Director
Rufus Britt
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
W. Chris Clark
Chief Financial Officer



COMMISSION
Gary C. Lemel
Chairman
Barry D. Malphrus
Vice Chairman
Robin B. Blackwood
Secretary
Eddie L. Miller
Stephanie M. Rawlinson
David L. Thomas

3440 Harden Street Extension
Columbia, South Carolina 29203
803/898-9600
Toll Free: 888/DSN-INFO
Home Page: www.ddsn.sc.gov

Reference Number: 567-04-DD

Title of Document: DDSN Approved Crisis Prevention Curricula List and Curriculum Approval Process

Date of Issue: January 1, 2009
Effective Date: January 1, 2009
Last Review Date: November 19, 2020
Date of Last Revision: November 19, 2020 **(REVISED)**

Applicability: DDSN Regional Centers, DDSN Operated Community Settings, DSN Boards, Adult Companion Providers, Day Service Providers (Career Prep, Day Activity, Community Services, Support Center), Early Intervention Providers, Employment Service Providers, Intermediate Care Facilities for Individuals with Intellectual Disabilities (ICFs/IID), Residential Habilitation Providers and Respite Providers

PURPOSE

This document establishes the requirement for all South Carolina Department of Disabilities and Special Needs (DDSN) operated programs (DDSN Regional Centers and DDSN Operated Community Settings), DSN Boards, and Contract Service Providers to choose and utilize a validated, competency-based curriculum or system for teaching and certifying staff to prevent and respond to disruptive behavior and crisis situations.

This document also establishes the requirement for the DDSN approval of curricula and includes procedures for submission of curricula to DDSN for review.

POLICY

Any system utilized to prevent and respond to disruptive behavior and crisis situations must reflect the values and principles of DDSN. A Crisis Prevention Management Curriculum is only approved once it has been determined that it aligns with DDSN philosophies and it has a strong focus of training in the area of interpersonal skills (e.g., active listening, problem solving, negotiation, and conflict management). In addition, DDSN prohibits training curricula that include techniques involving the use of force (such as chokeholds that would cut off air in any form that would prevent breathing, prone restraints or other techniques that inhibit breathing etc.) for self-defense or control that entities such as law enforcement would utilize.

Only the techniques included in the approved system/curriculum shall be used. Techniques included in the chosen system/curriculum shall only be employed by staff members who have been fully trained and deemed competent in the application of the techniques. The use of techniques not included in the chosen system/curriculum including homemade techniques or placing hands on someone in anyway, and/or the application of techniques by untrained staff shall constitute abuse.

Staff members (professional and paraprofessional) who provide direct support/services or supervise those who provide direct supports/services must be certified in the system chosen before performing the skill (refer to DDSN Directive 567-01-DD: Employee Orientation, Pre-service and Annual Training Requirements). When those supported are present and under the supervision of staff, at least one staff member who is certified in the chosen system must be present. By present, staff who are certified must, at a minimum, be within a five (5) minute response time of any who are not certified. Certified staff must be clearly identified and known to non-certified staff so, if needed, assistance can be obtained.

Neither this directive nor the content of the chosen curriculum in any way affects the requirements for individualized Behavior Support Plans (Refer to DDSN Directive 600-05-DD: Behavior Support, Psychotropic Medications and Prohibited Practices). The techniques employed by a chosen system are for use during emergency situations when no Behavior Support Plan has been designed (i.e., unpredictable occurrences) or when the current Behavior Support Plan fails to protect those involved from harm. In the event a person's Behavior Support Plan and the crisis response techniques within are unable to safely manage the situation, staff may call 911.

APPROVED CURRICULA

Only the systems/curricula listed below have been approved for use by DDSN:

1. The Mandt System®
2. CPI – Crisis Prevention Institute
3. PCM – Professional Crisis Management

4. Therapeutic Options Training Curriculum
5. PCS Life Experience Model
6. TCI – Therapeutic Crisis Intervention System
7. Safety-Care
8. Ukeru Systems

This directive will be updated when additional systems/curricula are approved. Any system on the list may be selected for use. Appropriate use of an approved system/curriculum includes competency-based assessment of employee skills and re-certification on the schedule required by the system/curriculum for trainers and staff.

When a system or curriculum that has not previously been approved is desired, the board/provider must submit to DDSN Central Office, Intellectual Disabilities/Related Disabilities Division a request that includes the name of the system for which approval is sought and either information about the system or a Web-address where system information can be located. Once information is reviewed, the board/provider will be notified of the decision in writing.

Barry D. Malphrus
Vice-Chairman

Gary C. Lemel
Chairman

Reference Number:	604-04-DD
Title of Document	Standard First Aid with Cardiopulmonary Resuscitation (CPR) – Adult, Child, Infant
Date of Issue:	May 21, 1990
Effective Date:	May 21, 1990
Last Review Date:	April 6, 2016 XXXX, 2020
Date of Last Revision:	April 6, 2016 XXXX, 2020 (REVISED)
Applicability:	DDSN Central Office, DDSN Regional Centers, DSN Boards and Contracted Service Providers

PURPOSE

This document establishes the minimum requirements for certification and recertification in first aid and cardiopulmonary resuscitation as well as minimum requirements for assuring safety when staff are not certified. These requirements are applicable, at a minimum to direct support staff and those who supervise direct support staff, Public Safety Officers and Administrative Officers of the Day (AOD's).

DEFINITIONS

Direct support staff are those employees or contract workers whose job descriptions indicate the duty of providing direct services/supports to individuals who receive DDSN sponsored services.

Certification in first aid includes skills such as splinting, controlling bleeding and caring for a variety of sudden illnesses.

Certification in CPR includes competency in conscious and unconscious choking, and CPR for adults, children, and infants.

Certification requirements are as defined by nationally recognized organizations (e.g., American Red Cross, American Heart Association, National Safety Council).

REQUIREMENTS

First Aid

DDSN Directive 567-01-DD: Employee Orientation, Pre-Service and Annual Training Requirements, establishes the minimum training requirements for employees including First Aid. When individuals are in the care of the staff, at least one (1) staff person who is certified in first aid must be present and clearly identified to non-certified staff. “Present” means staff who are certified must, at a minimum, be within a two (2) minute response time so assistance can be obtained immediately.

Re-certification must be completed without lapse according to the guidelines determined by the organization whose program is being utilized. If not re-certified prior to expiration of the previous certification period, evidence must be available to show that certified staff were present as services/supports were provided by the non-certified staff.

Cardiopulmonary Resuscitation (CPR)

DDSN Directive 567-01-DD: Employee Orientation, Pre-Service and Annual Training Requirements, establishes the minimum training requirements for employees, including CPR. When individuals are present and in the care of staff, at least one (1) staff who is certified in CPR must be present and clearly identified to non-certified staff. “Present” means staff who are certified must, at a minimum, be within a two (2) minute response time so assistance can be obtained immediately.

Re-certification must be completed without lapse in accordance with the guidelines established by the organization whose program is being utilized. If not re-certified prior to expiration of the previous certification period, evidence must be available to show that certified staff were present as services were provided by the non-certified staff.

Staff who provide direct services and supports to infants and/or children must be certified in Infant/Child CPR (Adult CPR alone is not sufficient). If not certified in Infant/Child CPR, when an infant or child is present and in the care of staff, at least one (1) staff certified in Infant/Child CPR must be present and clearly identified to non-certified staff so assistance can be obtained immediately. “Present” means staff who are certified must, at a minimum, be within a two (2) minute response time so assistance can be obtained immediately.

~~Susan Kreh Beck, Ed.S., NCSP
Associate State Director Policy
(Originator)~~

~~Beverly A.H. Buseemi, Ph.D.
State Director
(Approved)~~

Mary Poole
State Director
Patrick Maley
Deputy Director
Rufus Britt
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
W. Chris Clark
Chief Financial Officer



3440 Harden Street Extension
Columbia, South Carolina 29203
803/898-9600
Toll Free: 888/DSN-INFO
Home Page: www.ddsn.sc.gov

COMMISSION
Gary C. Lemel
Chairman
Barry D. Malphrus
Vice Chairman
Robin B. Blackwood
Secretary
Eddie L. Miller
Stephanie M. Rawlinson
David L. Thomas

Reference Number:	604-04-DD
Title of Document	Standard First Aid with Cardiopulmonary Resuscitation (CPR) – Adult, Child, Infant
Date of Issue:	May 21, 1990
Effective Date:	May 21, 1990
Last Review Date:	November 19, 2020
Date of Last Revision:	November 19, 2020 (REVISED)
Applicability:	DSN Boards and Contracted Service Providers, DDSN Operated Community Settings

PURPOSE

This document establishes the minimum requirements for certification and recertification in first aid and cardiopulmonary resuscitation as well as minimum requirements for assuring safety when staff are not certified. These requirements are applicable, at a minimum to direct support staff and those who supervise direct support staff, Public Safety Officers and Administrative Officers of the Day (AOD's).

DEFINITIONS

Direct support staff are those employees or contract workers whose job descriptions indicate the duty of providing direct services/supports to individuals who receive DDSN sponsored services.

Certification in first aid includes skills such as splinting, controlling bleeding and caring for a variety of sudden illnesses.

Certification in CPR includes competency in conscious and unconscious choking, and CPR for adults, children, and infants.

Certification requirements are as defined by nationally recognized organizations (e.g., American Red Cross, American Heart Association, National Safety Council).

REQUIREMENTS

First Aid

DDSN Directive 567-01-DD: Employee Orientation, Pre-Service and Annual Training Requirements, establishes the minimum training requirements for employees including First Aid. When individuals are in the care of the staff, at least one (1) staff person who is certified in first aid must be present and clearly identified to non-certified staff. "Present" means staff who are certified must, at a minimum, be within a two (2) minute response time so assistance can be obtained immediately.

Re-certification must be completed without lapse according to the guidelines determined by the organization whose program is being utilized. If not re-certified prior to expiration of the previous certification period, evidence must be available to show that certified staff were present as services/supports were provided by the non-certified staff.

Cardiopulmonary Resuscitation (CPR)

DDSN Directive 567-01-DD: Employee Orientation, Pre-Service and Annual Training Requirements, establishes the minimum training requirements for employees, including CPR. When individuals are present and in the care of staff, at least one (1) staff who is certified in CPR must be present and clearly identified to non-certified staff. "Present" means staff who are certified must, at a minimum, be within a two (2) minute response time so assistance can be obtained immediately.

Re-certification must be completed without lapse in accordance with the guidelines established by the organization whose program is being utilized. If not re-certified prior to expiration of the previous certification period, evidence must be available to show that certified staff were present as services were provided by the non-certified staff.

Staff who provide direct services and supports to infants and/or children must be certified in Infant/Child CPR (Adult CPR alone is not sufficient). If not certified in Infant/Child CPR, when an infant or child is present and in the care of staff, at least one (1) staff certified in Infant/Child CPR must be present and clearly identified to non-certified staff so assistance can be obtained immediately. "Present" means staff who are certified must, at a minimum, be within a two (2) minute response time so assistance can be obtained immediately.

Barry D. Malphrus
Vice Chairman

Gary C. Lemel
Chairman

Reference Number:	367-02-DD
Title of Document:	Acquiring Information Technology (IT) Products and Services
Date of Issue:	May 1, 1987
Effective Date:	May 1, 1987
Last Review Date:	April 19, 2016 XXXX, 2020
Date of Last Revision:	April 19, 2016 XXXX, 2020 (REVISED)
Applicability:	DDSN Central Office; DDSN District Offices and DDSN Regional Centers, <u>DDSN Operated Community Settings</u>

I. Purpose

The purpose of this directive is to establish uniform policies and procedures for acquiring Information Technology (IT) hardware, software, training, consulting and services. This directive encompasses all ~~IT Information Technology~~ procured through a purchase, rental agreement, or a lease. A uniform policy is necessary to ensure ~~IT information technology~~ is identified, evaluated and procured in the most cost-effective and efficient manner.

II. General Policies

- A. It is mandatory that all IT products and services be compatible with the hardware and software standards as established by the ~~Director of the Information Technology Division~~ Chief Information Officer (CIO).
- B. All consumable items, such as: toner cartridges, printer maintenance kits, minor computer accessories, and analog telephones require the appropriate departmental approvals prior to purchase and do not require expressed approval by the CIO.
- C. Prior to the actual purchase, all non-consumable IT products and services must be evaluated by the Division of Information Technology to ensure compliance with all IT

established security and technical standards. The CIO and the Chief Information Security Officer (CISO) will collaborate when necessary on the review of technology purchases; to ensure CISO has review opportunity for compliance and security standards.

- D. All non-consumable IT information technology procurements (hardware and software) purchases require the prior approval of the ~~Director of the Information Technology Division~~CIO or ~~his~~their designee. This includes printers whether they are multifunction, laser jet, or desk jet devices. Approval is also required whether the devices are purchased, rented, or leased.

~~Consumable items, such as: toner cartridges; printer maintenance kits; CD's; floppy disks; tapes; ink jet cartridges, and analog telephone do not require approval.~~

III. Processing Procedures

- A. ~~A.~~—All requests for non-consumable IT products and services must be initiated by submitting a properly completed ~~submitted on an~~ “Information Technology Procurement Request,” form to the ~~Director of the Information Technology Division~~CIO. All signatures must be obtained as required on the form. ~~The form must be filled out completely and have the approval of the appropriate Regional IT Coordinator.~~ The Division of Information Technology should be consulted for assistance in the completion of the form.

- B. If the acquisition of IT products or services are to be achieved through entering into a lease or rental agreement, then the proposed agreement must be provided with the request for purchase. If there are support, maintenance, licensing, or other agreements to be entered into, then these documents must also be provided with the request for purchase.

- A.C. If approved by the ~~CIO~~Director of the Information Technology, the IT Procurement Request will be forwarded to the Central Office Purchasing and Supply Agency Procurement department for processing. All purchase orders for IT products and services must be issued by Central Office Purchasing.

- B.D. The Division of Information Technology will monitor the procurement, approve receipt, and coordinate installation of all IT products and services.

~~Tom Waring~~Barry D. Malphrus
~~Associate State Director Administration~~
~~Vice Chairman~~

~~Beverly Buscemi, Ph.D.~~Gary C. Lemel
~~State Director~~ Chairman

To access the following attachments, please see the agency website page “Current Directives” at: <https://ddsn.sc.gov/providers/ddsn-directives-standards-and-manuals/current-directives>

Attachment: Information Technology Procurement Request Form

Mary Poole
State Director
Patrick Maley
Deputy Director
Rufus Britt
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
W. Chris Clark
Chief Financial Officer



COMMISSION
Gary C. Lemel
Chairman
Barry D. Malphrus
Vice Chairman
Robin B. Blackwood
Secretary
Eddie L. Miller
Stephanie M. Rawlinson
David L. Thomas

3440 Harden Street Extension
Columbia, South Carolina 29203
803/898-9600
Toll Free: 888/DSN-INFO
Home Page: www.ddsn.sc.gov

Reference Number: 367-02-DD

Title of Document: Acquiring Information Technology (IT) Products and Services

Date of Issue: May 1, 1987
Effective Date: May 1, 1987
Last Review Date: November 19, 2020
Date of Last Revision: November 19, 2020 (REVISED)

Applicability: DDSN Central Office and DDSN Regional Centers, DDSN Operated Community Settings

I. Purpose

The purpose of this directive is to establish uniform policies and procedures for acquiring Information Technology (IT) hardware, software, training, consulting and services. This directive encompasses all IT procured through a purchase, rental agreement, or a lease. A uniform policy is necessary to ensure IT is identified, evaluated and procured in the most cost-effective and efficient manner.

II. General Policies

- A. It is mandatory that all IT products and services be compatible with the hardware and software standards as established by the Chief Information Officer (CIO).
- B. All consumable items, such as: toner cartridges, printer maintenance kits, minor computer accessories, and analog telephones require the appropriate departmental approvals prior to purchase and do not require expressed approval by the CIO.

- C. Prior to the actual purchase, all non-consumable IT products and services must be evaluated by the Division of Information Technology to ensure compliance with all IT established security and technical standards. The CIO and the Chief Information Security Officer (CISO) will collaborate when necessary on the review of technology purchases to ensure CISO has review opportunity for compliance and security standards.
- D. All non-consumable IT (hardware and software) purchases require the prior approval of the CIO or their designee. This includes printers whether they are multifunction, laser jet, or desk jet devices. Approval is also required whether the devices are purchased, rented, or leased.

III. Processing Procedures

- A. All requests for non-consumable IT products and services must be initiated by submitting a properly completed “Information Technology Procurement Request,” form to the CIO. All signatures must be obtained as required on the form. The Division of Information Technology should be consulted for assistance in the completion of the form.
- B. If the acquisition of IT products or services are to be achieved through entering into a lease or rental agreement, then the proposed agreement must be provided with the request for purchase. If there are support, maintenance, licensing, or other agreements to be entered into, then these documents must also be provided with the request for purchase.
- C. If approved by the CIO, the IT Procurement Request will be forwarded to the Agency Procurement department for processing. All purchase orders for IT products and services must be issued by Central Office Purchasing.
- D. The Division of Information Technology will monitor the procurement, approve receipt, and coordinate installation of all IT products and services.

Barry D. Malphrus

Gary C. Lemel Chairman Vice Chairman

To access the following attachments, please see the agency website page “Current Directives” at: <https://ddsn.sc.gov/providers/ddsn-directives-standards-and-manuals/current-directives>

Attachment: Information Technology Procurement Request Form

Mary Poole
State Director
Patrick Maley
Deputy Director
Rufus Britt
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
W. Chris Clark
Chief Financial Officer



3440 Harden Street Extension
 Columbia, South Carolina 29203
 803/898-9600
 Toll Free: 888/DSN-INFO
 Home Page: www.ddsn.sc.gov

COMMISSION
Gary C. Lemel
Chairman
Barry D. Malphrus
Vice Chairman
Robin B. Blackwood
Secretary
Eddie L. Miller
Stephanie M. Rawlinson
David L. Thomas

Reference Number: 367-32-DD

Title of Document: Information Security and Privacy

Date of Issue: November 19, 2020
 Effective Date: November 19, 2020
 Last Review Date: November 19, 2020
 Date of Last Revision: November 19, 2020 (NEW)

Applicability: DDSN Employees, DDSN Operated Community Settings,
 DSN Boards and Contracted Service Providers

PURPOSE

The purpose of this directive is to set forth the South Carolina Department of Disabilities and Special Needs' (DDSN) Information Security and Privacy policy requirements consistent with South Carolina state law contained in recurring Provisos 117.113 (2014) and 101.32 (2014) and any successive statutes. State law requires all South Carolina state agencies, including institutions, departments, divisions, boards, commissions, and authorities, to implement the South Carolina Division of Information Security's Information Security and Privacy Standards, commonly identified as [SCDIS-200](#).

BACKGROUND

Within statutory scope, these SCDIS-200 Standards apply to:

- All persons managed by an agency, such as employees, contractors, and volunteers.
- All agency information systems, regardless of location or service level agreement.
- All information contained on any agency information system, regardless of format or medium.

- All information otherwise under the control of any agency, regardless of format or medium.

The SCDIS-200 is comprised of 343 information and privacy control requirements for state agencies to implement. The South Carolina Division of Information Security organized these 343 requirements into 13 “control family” templates for state agency use to set out a logical framework for agencies to implement requirements.

POLICY

The DDSN has adopted and must implement the SCDIS-200 Standards in their entirety unless a business risk acceptance has been fully documented and approved by the State Director.

DDSN’s Information Security Office will develop information security and privacy procedures to implement SCDIS-200 Standards to protect the availability, integrity, and confidentiality of DDSN Information Technology (IT) resources. While these directives apply to all staff, they are primarily applicable to Data Stewards; those managing the access to data and IT resources; and those using DDSN IT resources.

DDSN adopts the South Carolina Division of Information Security’s 13 “control family” requirement templates (Appendices A-M) and added two additional requirement documents (Appendices N and O) to be used as the operating framework to meet minimum SCDIS-200 Standards. These requirement documents are contained in the following Appendices:

<u>Appendix Number</u>	<u>Document Description</u>	<u>Page Number</u>
Appendix A	Information Security - Program	4-8
Appendix B	Information Security - Access Control	9-18
Appendix C	Information Security - Asset Management	19
Appendix D	Information Security - Business Continuity Management	20-25
Appendix E	Human Resource and Security Awareness	26-27
Appendix F	Information Security Information Systems Acquisitions, Development, and Maintenance	28-33
Appendix G	Information Security - IT Compliance	34-36
Appendix H	Information Security - IT Risk Strategy	37-39
Appendix I	Mobile Device Security	40-41
	Mobile Device Access Agreement	42
Appendix J	Physical Access and Environmental Security	43-46
Appendix K	Information Security - Risk Management	47-49
Appendix L	Information Security - Threat and Vulnerability Management	50-53
Appendix M	Data Protection and Privacy	54-58
Appendix N	Acceptable Use of Network Services and the Internet	59-61
	Acceptable Use Policy Acknowledgement	62
Appendix O	Service Provider Data Protection (DSN Boards/Providers)	63-64

DDSN expects all employees and users to adhere to the requirements set forth in this directive as described fully in the attached appendices. No set of requirements can address all scenarios of IT security; therefore, these requirements address the most common aspects of information security.

IMPLEMENTATION, MAINTENANCE AND COMPLIANCE

1. DDSN's designated Chief Information Security Officer (CISO) is responsible for ensuring this directive is implemented and communicated throughout DDSN.
2. The CISO is responsible for ensuring that each control owner has developed operating procedures to implement all requirements. These operating procedures will be organized and made easily accessible to users, both internal to DDSN and the external provider network.
3. The CISO is responsible for ensuring compliance with SCDIS-200 requirements. The CISO will periodically, but no less than twice annually, provide a written report to executive management on the compliance status of all SCDIC-200 requirements, as well as provide a risk matrix (occurrence and consequence) of the control requirement families or other logical categorization of information security and privacy activity.
4. Any revisions to this directive shall be developed by the Information Security Office and follow the normal approval process according to DDSN Directive 100-01-DD: Electronic Communications Systems.
5. Violation of the provisions of approved requirements will be subject to disciplinary action in accordance with DDSN's progressive discipline policy.

Barry D. Malphrus
Vice Chairman

Gary C. Lemel
Chairman

APPENDIX A

Information Security - Program

1. Information Security Program Planning
 - a. Information Security Plan (PM 1)
 - i. DDSN shall develop and communicate an information security plan that underlines security requirements, the security management controls, and common controls in place for meeting those requirements.
 - ii. DDSN's security plan shall identify and assign security program roles, responsibilities, and management commitment, and ensure coordination among the agency's business units, as well as compliance with the security plan.
 - iii. DDSN shall ensure coordination among the agency's business units responsible for the distinct aspects of information security (i.e., technical, physical, personnel, etc.).
 - iv. DDSN shall ensure that the security plan is approved by senior management.
 - v. DDSN shall review the information security plan at least on an annual basis.
 - vi. DDSN shall update the security plan to address changes and problems identified during plan implementation or security control assessments.
 - vii. DDSN shall protect the information security plan from unauthorized disclosure and modification
 - b. Information Security Resources (PM 3)
 - i. DDSN shall consider resources needed to implement and maintain the information security plan in capital planning and investment requests.
 - c. Plan of Action and Milestones Process (PM 4)
 - i. DDSN shall implement a process for ensuring that plans of action and milestones for the security program and associated information systems are developed and maintained.
 - ii. DDSN shall review plans of action and milestones for consistency with the agency's risk management strategy and priorities for risk response actions.

- d. Information Security Measures of Performance (PM 6)
 - i. DDSN shall develop, monitor, and report on the results of information security measures of performance, as directed or guided by the South Carolina Division of Information Security (SCDIS) and the South Carolina Enterprise Privacy Office (SCEPO).
- e. Guidance:
 - i. NIST SP 800-53 Revision 4: PM 1 Information Security Program Plan
 - ii. NIST SP 800-53 Revision 4: PM 3 Information Security Resources
 - iii. NIST SP 800-53 Revision 4: PM 4 Plan of Action and Milestones Process
 - iv. NIST SP 800-53 Revision 4: PM 6 Measures of Performance

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

2. Security Organization (Roles and Responsibilities)

- a. Information Security Authority (2.2.3.1)
 - i. DDSN's chief executive shall ensure that the agency's senior officials are given the necessary authority to secure the operations and assets under their control.
- b. Information Security Liaison (PM 2)
 - i. DDSN shall appoint an information security liaison with the mission and resources to coordinate, develop, implement, and maintain an information security plan.
- c. Information Security Workforce (PM 13)
 - i. DDSN shall establish an information security workforce and professional development program appropriately sized to the agency's information security needs.
- d. Role-based Security Training (AT 3)
 - i. DDSN shall provide role-based security training to personnel with assigned security roles and responsibilities.
- e. Guidance:
 - i. NIST SP 800-53 Revision 4: PM 2 Senior Information Security Officer
 - ii. NIST SP 800-53 Revision 4: PM 13 Information Security Workforce
 - iii. NIST SP 800-53 Revision 4: AT 3 Role-based Security Training
 - iv. NIST SP 800-100: 2.2.3.1 Agency Head

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

3. Policy Management (Plan of Action)

a. Procedure Development

- i. DDSN shall adopt a risk-based approach to identify State, Federal and agency-specific information security objectives, and shall develop information security procedures in alignment with the identified security objectives.
- ii. DDSN shall allocate the appropriate subject matter experts to the development of State and agency-specific information security procedures.
- iii. DDSN shall approach independent external (third party) specialists to assist in the development of information security policies in cases where it is established that the required skills do not exist within the agency and are not available within any other state government agency.
- iv. DDSN shall work in collaboration with other states, Federal government, and external special interest groups in cases where procedures directly or indirectly affect interfacing activities with them.
- v. Information security procedures that are developed at the agency shall contain the following information, as appropriate:
 1. Revision history
 2. Introduction
 3. Preface
 4. Ownership, roles, and responsibilities
 5. Purpose
 6. Policy statements
 7. Policy supplement
 8. Guidance
 9. Definitions
- vi. Scenarios which cannot be effectively addressed within the constraints of the agency's security procedures, should be identified as exceptions:
 1. Exceptions shall be evaluated in the context of potential risk to the agency as a whole;
 2. Exceptions that create significant risks without adequate compensating controls shall not be approved; and
 3. Exceptions shall be consistently evaluated in accordance with the agency's risk acceptance practice.

- vii. DDSN shall review each draft procedure with stakeholders who shall be impacted by the procedure, to ensure that the procedure is enforceable and effective.
 - viii. DDSN shall identify gaps within the procedures that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps.
 - ix. DDSN shall develop and implement a communication plan to disseminate new procedures or changes to existing procedures.
 - x. DDSN shall review procedures on an annual basis to ensure that procedures are up-to-date and aligned with the State's risk posture.
 - b. Procedure Review and Approval
 - i. A procedure governance committee shall be established for the purpose of review and approval of procedures.
 - ii. Procedure exemptions shall be explicitly approved by the procedure governing committee.
 - iii. Procedure approval history shall be documented in detail.
 - c. Procedure Implementation
 - i. DDSN shall implement mechanisms to help ensure that information security procedures will be available to the agency's personnel on a continuous basis and whenever required.
 - ii. DDSN shall require employees to review and acknowledge understanding of information security procedures prior to allowing access to sensitive data or information systems.
 - d. Guidance:
 - i. NIST SP 800-53 Revision 4: PM 6 Measures of Performance

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>
- 4. Information Security Controls Deployment
 - a. Controls Deployment
 - i. DDSN shall adopt a risk-based approach to prioritize deployment of controls.

- ii. DDSN shall allocate the appropriate subject matter experts to the deployment of State, Federal and agency-specific information security controls.
- iii. DDSN shall approach independent external (third party) specialists to assist in the deployment of information security controls in cases where it is established that the required skills do not exist within the agency and are not available within any other state government agency.
- iv. Controls which cannot be deployed due to the agency's resource or other constraints must be reported to the office of the State Chief Information Security Officer.
- v. DDSN shall review each control with stakeholders who shall be impacted, to ensure that the control is enforceable and effective.
- vi. DDSN shall identify gaps within the controls that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps.
- vii. DDSN shall develop and implement a communication plan to disseminate new controls or changes to existing controls.
- viii. DDSN shall review controls on an annual basis to ensure that they are up-to-date and aligned with the State's risk posture.

APPENDIX B

Information Security - Access Control

1. Access Management
 - a. The purpose of the access management section is to establish processes to control access and use of DDSN information resources. Access management incorporates role-based access controls (RBAC), privileged user access, access definitions, roles, and profiles.
 - b. Access Control Policy and Procedures (AC 1)
 - i. DDSN shall establish formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
 - c. Account Management (AC 2)
 - i. DDSN shall identify account types (e.g., individual, group, system, application, guest/anonymous, and temporary) and establish conditions for group membership.
 - ii. DDSN shall identify authorized users of information systems and specify access rights.
 - iii. Requests for access to DDSN Data must be approved by the business/data owner (or delegate) prior to provisioning the user account.
 - iv. DDSN shall authorize and monitor the use of guest/anonymous and temporary accounts, and notify relevant personnel (e.g., account managers) when temporary accounts are no longer required.
 - v. DDSN shall utilize request for access change documentation (e.g., account managers, system administrators) to remove or deactivate access rights when users are terminated, transferred, or access rights requirements change.
 - vi. DDSN shall remove or disable default user accounts and, if user accounts cannot be removed or disabled, they should be renamed.
 - vii. Access shall be granted based upon the principles of need-to-know, least-privilege, and separation of duties. Access not explicitly permitted shall be denied by default.

- viii. Access requests from users shall be recorded and follow the DDSN established approval process.
 - ix. DDSN shall ensure that user access requests are approved by a business owner (or any other pre-approved role).
 - x. Privileged accounts (e.g., system/network administrators having root level access, database administrators), shall only be allowed after approval by a DDSN information security officer and/or similarly designated role. The approval shall be granted to a limited number of individuals with the requisite skill, experience, business need, and documented reason based on role requirements.
 - xi. DDSN shall ensure that privileged accounts are controlled, monitored, and can be reported on a periodic basis.
 - xii. DDSN shall enforce periodic user access reviews to be performed by information/data owners or their assigned delegate(s) to ensure the following:
 - 1. Access levels remain appropriate, based upon approvals;
 - 2. Terminated employees do not have active accounts;
 - 3. There are no group accounts, unless approved; and
 - 4. There are no duplicate user identifiers.
 - xiii. DDSN shall review information system accounts within every 180 days and require annual certification.
 - xiv. DDSN shall regulate information system access and define security requirements for contractors, vendors, and other service providers.
 - xv. DDSN shall administer privileged user accounts in accordance with a role-based access model.
- d. Access Enforcement (AC 3)
- i. DDSN shall enforce approved authorizations for logical access to information systems.
 - ii. DDSN shall implement encryption as an access control mechanism if required by Federal, State, or other laws or regulations.
- e. Information Flow Enforcement (AC 4)
- i. For Restricted data: DDSN systems shall enforce data flow controls using security attributes on information, source, and destination objects as a basis for flow control decisions.

- f. Separation of Duties (AC 5)
 - i. DDSN shall implement controls in information systems to enforce separation of duties through assigned access authorizations, including but not limited to:
 - 1. Audit functions are not performed by security personnel responsible for administering information system access;
 - 2. Divide critical business and information system management responsibilities;
 - 3. Divide information system testing and production functions between different individuals or groups; and
 - 4. Independent entity to conduct information security testing of information systems.
 - ii. DDSN shall document and implement separation of duties through assigned information system access authorizations.
- g. Least Privilege (AC 6)
 - i. DDSN shall ensure that only authorized individuals have access to DDSN data/information and that such access is strictly controlled, audited in accordance with the concepts of “need-to-know, least-privilege, and separation of duties.”
 - ii. DDSN shall implement processes or mechanisms to:
 - 1. Disable file system access not explicitly required for system, application, and administrator responsibilities;
 - 2. Provide minimal physical and system access to the contractors and ensure information security policy adherence by all contractors;
 - 3. Restrict use of database management to authorized database administrators;
 - 4. Grant access to authorized users based on their required job duties; and
 - 5. Disable all system and removable media boot access unless explicitly authorized by the CIO; if authorized, boot access shall be password protected.
- h. Unsuccessful Login Attempts (AC 7)
 - i. DDSN systems shall enforce a limit of unsuccessful logon attempts during a DDSN-defined period. The number of logon attempts shall be commensurate with the classification of data hosted, processed, or transferred by the information system.

- ii. DDSN shall automatically lock user accounts the after maximum logon attempts is reached. DDSN shall establish an account lock time period commensurate with the classification of data hosted, processed, or transferred by the information system.
- i. System Use Notification (AC 8)
 - i. DDSN systems shall display the following warning before granting system access. “This system is solely for the use of authorized DDSN personnel. The information contained herein is the property of DDSN and subject to non-disclosure, security, and confidentiality requirements. DDSN shall monitor system usage for unauthorized activities. Any user accessing this system expressly consents to such monitoring.”
- j. Session Lock (AC 11)
 - i. DDSN systems shall time out sessions or require a re-authentication process after 30 minutes or less of inactivity.
- k. Guidance:
 - i. NIST SP 800-53 Revision 4: AC 1 Access Control Policy and Procedures
 - ii. NIST SP 800-53 Revision 4: AC 3 Access Enforcement
 - iii. NIST SP 800-53 Revision 4: AC 4 Information Flow Enforcement
 - iv. NIST SP 800-53 Revision 4: AC 5 Separation of Duties
 - v. NIST SP 800-53 Revision 4: AC-6 Least Privilege
 - vi. NIST SP 800-53 Revision 4: AC 7 Unsuccessful Login Attempts
 - vii. NIST SP 800-53 Revision 4: AC 8 System Use Notification
 - viii. NIST SP 800-53 Revision 4: AC 11 Session Lock

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

2. Network Access Management

- a. Remote Access (AC 17)
 - i. DDSN shall document allowed methods for remote access to the network and information systems.
 - ii. DDSN shall utilize automated mechanisms to enable management to monitor and control remote connections into networks and information systems.
 - iii. Virtual Private Network (VPN) or equivalent encryption technology shall be used to establish remote connections with DDSN networks and information systems.

- iv. Remote users shall connect to DDSN information systems only using mechanism protocols approved by the DDSN through a limited number of managed access control points for remote connections.
 - v. For Restricted data and/or system administrators: DDSN employees and authorized third parties accessing DDSN information systems remotely shall do so via an approved two-factor authentication (2FA) technology.
 - vi. DDSN shall develop formal procedures for authorized individuals to access its information systems from external systems, such as access allowed from an alternate work site (if required).
- b. Wireless Access (AC 18)
- i. DDSN establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
 - ii. DDSN shall only use wireless networking technology that enforces user authentication.
 - iii. DDSN shall authorize wireless access to information systems prior to allowing use of wireless networks.
 - iv. DDSN does not allow wireless access points to be installed independently by users.
- c. Use of External Information Systems (AC 20)
- i. If external systems are authorized by the DDSN, the DDSN shall establish terms and conditions for their use, including types of applications that can be accessed from external information systems, security category of information that can be processed, stored, and transmitted, use of VPN and firewall technologies, the use and protection against the vulnerabilities of wireless technologies, physical security maintenance and the security capabilities of installed software are to be updated.
- d. Boundary Protection (SC 7)
- i. DDSN networks where information deemed critical by DDSN is stored or processed shall be physically or logically segregated from publicly available networks.
 - ii. DDSN networks and information systems shall not be accessible from public networks (e.g., Internet) except under secured and managed interfaces employing boundary protection devices.

- iii. DDSN limits network access points to a minimum to enable effective monitoring of inbound and outbound communications and network traffic.
- e. Guidance:
 - i. NIST SP 800-53 Revision 4: AC 17 Remote Access
 - ii. NIST SP 800-53 Revision 4: AC 18 Wireless Access
 - iii. NIST SP 800-53 Revision 4: AC 20 Use of External Information Systems
 - iv. NIST SP 800-53 Revision 4: SC 7 Boundary Protection

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

3. Identity Management

- a. Identification and Authentication (IA 2, IA 4, AND IA 8)
 - i. DDSN shall establish processes to enforce the use of unique system identifiers (User IDs) assigned to each user, including technical support personnel, system operators, network administrators, system programmers, and database administrators.
 - ii. DDSN shall prevent reuse of user identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier.
 - iii. DDSN shall allow the use of group IDs only where these are necessary for business or operational reasons; group IDs shall be formally approved and documented.
 - iv. If DDSN requires group IDs, it shall require individuals to be authenticated with a unique user account prior to using the group ID (e.g., network authentication prior to use of Group ID).
 - v. DDSN shall minimize the use of system, application, or service accounts; and DDSN shall document, formally approve, and designate a responsible party of this type of accounts.
 - vi. DDSN security system shall be able to identify and verify the identification and, if deemed necessary by DDSN, the location of each authorized user.
- b. Guidance:
 - i. NIST SP 800-53 Revision 4: IA 2 Identification and Authentication (Organizational Users)
 - ii. NIST SP 800-53 Revision 4: IA 4 Identifier Management

- iii. NIST SP 800-53 Revision 4: IA 8 Identification and Authentication (Non-Organizational Users)

To access any Guidance references, please see the attached link at:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

4. Authentication

- a. Authenticator Management (IA 5)
 - i. DDSN shall choose a suitable multifactor authentication technique to substantiate the claimed identity of a user.
- b. Unsuccessful Logon Attempts (AC 7)
 - i. DDSN shall implement mechanisms to record successful and failed authentication attempts.
- c. Session Lock (AC 11)
 - i. DDSN shall define a maximum number of invalid logon attempts commensurate to the criticality of network or information systems.
 - ii. DDSN networks and information systems shall disable user access upon reaching the maximum number of invalid access attempts as defined by the DDSN.
 - iii. Network and information systems sessions should remain locked for a predetermined time or until the user reestablishes access through an established authentication procedure.
- d. Guidance:
 - i. NIST SP 800-53 Revision 4: AC 7 Unsuccessful Logon Attempts
 - ii. NIST SP 800-53 Revision 4: AC 11 Session Lock
 - iii. NIST SP 800-53 Revision 4: IA 5 Authenticator Management

To access any Guidance references, please see the attached link at:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

5. Emergency Access

- a. Policy Account Management (AC 2)
 - i. DDSN shall establish processes and procedures for users to obtain access to required information systems on an emergency basis.

- ii. The emergency procedures shall ensure that:
 - 1. Only identified and authorized personnel are allowed access to live systems and data;
 - 2. All emergency actions are documented in detail; and
 - 3. Emergency action is reported to management and reviewed in an orderly manner.
- iii. DDSN will establish a process to automatically terminate emergency accounts within 24 hours and temporary accounts with a fixed duration not to exceed 365 days.

b. Guidance:

- i. NIST SP 800-53 Revision 4: AC 2 Account Management

To access any Guidance references, please see the attached link at:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

6. Password Policy

a. Account Management (AC 2)

- i. DDSN shall establish a process for password-based authentication to include the following:
 - 1. Automatically force users (including administrators) to change user account passwords every 90 days.
 - 2. Automatically force system administrators (including database, network, and application administrators) to change user account passwords no less than every 60 days.
 - 3. Passwords for system accounts to be changed at least every 180 days.
 - 4. Enforce password minimum lifetime of one (1) day.
 - 5. Prohibit the use of dictionary names or words as passwords.
 - 6. Enforce password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lowercase letters, and numbers) and/or special characters.
 - 7. Enforce a minimum number of characters to be changed when new passwords are created. For Restricted data consider a minimum of four (4) changed characters.
 - 8. Encrypt passwords in storage and during transmission.
 - 9. Prohibit password reuse for six (6) generations prior to reuse.
- ii. DDSN users shall not share passwords with others under any circumstance.

- iii. System passwords shall be changed immediately upon termination/resignation of any employee with privileged access.
- iv. DDSN shall not allow users to use common words or based on personal information as passwords (e.g., username, social security number, children's names, pets' names, hobbies, anniversary dates, etc.).
- v. DDSN shall suspend user accounts after a specified number of days of inactivity.
- vi. DDSN shall implement a process to change passwords immediately if there is reason to believe a password has been compromised or disclosed to someone other than the authorized user.

b. Guidance:

- i. NIST SP 800-53 Revision 4: AC 2 Account Management

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

7. Password Administration

a. Policy Access Agreements (PS 6)

- i. DDSN users shall sign an acknowledgement to evidence understanding of authentication policies, including the DDSN policy to keep passwords confidential and to keep group passwords solely within the members of the group.
- ii. DDSN shall require that employees sign acknowledgement prior to allowing access to network and information systems.

b. Identification and Authentication (IA 2, IA 6, and IA 8)

- i. DDSN shall establish a process to verify the identity of a user prior to providing a new, replacement or temporary password.
- ii. DDSN shall establish a process to uniquely identify and authenticates non-Agency users.
- iii. DDSN shall establish procedures to manage new or removed privileged accounts passwords.

c. Authenticator Management (IA 5)

- i. First-time passwords shall be set to a unique value per user and changed immediately after first use.

- ii. DDSN shall provide temporary passwords to users in a secure manner; the use of third parties or unprotected (i.e., clear text) electronic mail messages shall be prohibited.
 - iii. DDSN shall not allow default passwords for network and remote applications.
- d. Authenticator Feedback (IA 6)
- i. DDSN shall obscure feedback of authentication information during the authentication process to protect the information from exploitation/use by unauthorized individuals.
- e. Guidance:
- i. NIST SP 800-53 Revision 4: IA 2 Identification and Authentication (Organizational Users)
 - ii. NIST SP 800-53 Revision 4: IA 5 Authenticator Management
 - iii. NIST SP 800-53 Revision 4: IA 6 Authenticator Feedback
 - iv. NIST SP 800-53 Revision 4: IA 8 Identification and Authentication (Non-Organizational Users)
 - v. NIST SP 800-53 Revision 4: PS 6 Access Agreements

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

APPENDIX C

Information Security - Asset Management

1. Access Identification
 - a. Information System Component Inventory (CM 8)
 - i. DDSN shall document and maintain inventories of the important assets associated with each information system. Asset inventories shall include a unique system name, a system/business owner, a data classification, and a description of the location of the asset. Examples of assets associated with information systems are:
 1. Information assets: databases and data files, system documentation, user manuals, training material, operational procedures, disaster recovery plans, archived information.
 2. Software assets: application software, system software, development tools and utilities.
 3. Physical assets: physical equipment (e.g., processors, monitors, laptops, portable devices, tablets, smartphones), communication equipment (e.g., routers, servers), magnetic media (e.g., tapes and disks).
 4. Services: computing and communications services.
 - ii. Access to DDSN assets shall be requested via a formal registration process that requires user acknowledgement of all rules and regulations pertinent to the asset.
 - iii. DDSN shall periodically revalidate the asset to ensure that it is classified appropriately and that the safeguards remain valid and operative.
 - b. Security Impact Analysis (CM 4)
 - i. DDSN shall classify assets into the data classification types in the State of South Carolina Data Classification Schema.
 - ii. DDSN shall ensure that each asset is classified based on data classification type and impact level, and the appropriate level of information security safeguards are available and in place.
 - c. Guidance:
 - i. NIST SP 800-53 Revision 4: CM 4 Security Impact Analysis
 - ii. NIST SP 800-53 Revision 4: CM 8 Information System Component Inventory

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

APPENDIX D

Information Security - Business Continuity Management

1. Contingency Planning
 - a. Contingency Planning Policy and Procedures (CP 1)
 - i. DDSN shall establish a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
 - ii. DDSN shall establish formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
 - iii. DDSN shall establish a formal process for annual contingency planning policy and procedure review and update.
 - b. Contingency Plan (CP 2, CP 7)
 - i. DDSN shall conduct a Business Impact Analysis (BIA) to identify functions, processes, and applications that are critical to the DDSN and determine a point in time (i.e., recovery time objective (RTO)) when the impact of an interruption or disruption becomes unacceptable to the DDSN.
 - ii. DDSN shall utilize the BIA results to determine potential impacts resulting from the interruption or disruption of critical business functions, processes, and applications.
 - iii. DDSN shall assign contingency roles and responsibilities to key individuals from all business functions.
 - iv. DDSN shall establish procedures to maintain continuity of critical business functions despite critical information system disruption, breach, or failure.
 - v. DDSN shall document a Business Continuity Plan (BCP) that addresses documented recovery strategies designed to enable the DDSN to respond to potential disruptions and recover its critical business functions within a predetermined RTO following a disruption.
 - vi. DDSN shall establish a process to ensure that the BCP is reviewed and approved by senior management.

- vii. DDSN shall distribute copies of the BCP to key personnel responsible for the recovery of the critical business functions and other relevant personnel and partners with contingency roles, as determined by the DDSN.
 - viii. DDSN shall establish and implement procedures to review the BCP at planned intervals and at least on an annual basis.
 - ix. DDSN shall establish a process to update the contingency plan, including BIA, when changes to the organization, information system, or environment of operation occurred.
- c. Contingency Training (CP 3)
- i. DDSN shall provide training to personnel with assigned contingency roles and responsibilities.
 - ii. DDSN shall establish a process for identifying and delivering training requirements (i.e., frequency) to and from the relevant participants and evaluating the effectiveness of its delivery.
 - iii. DDSN shall incorporate simulated events and lessons learned into contingency training to facilitate effective response by personnel with contingency roles when responding to disruption.
- d. Contingency Plan Testing (CP 4)
- i. DDSN shall test the BCP at least annually to determine the effectiveness of the plan and the DDSN readiness to execute the plan.
 - ii. DDSN shall review the BCP test results, record lessons learned and perform corrective actions as needed.
 - iii. DDSN shall employ standard testing methods, ranging from walk-through and tabletop exercises to more elaborate parallel/full interrupt simulations, to determine the effectiveness of the plan and to identify potential weaknesses in the plans.
- e. Criticality Analysis (SA 14)
- i. DDSN shall establish procedures to enable continuation of critical business operations while operating in emergency mode.
- f. Guidance:
- i. NIST SP 800-53 Revision 4: CP 1 Contingency Planning Policy and Procedures

- ii. NIST SP 800-53 Revision 4: CP 2 Contingency Plan
- iii. NIST SP 800-53 Revision 4: CP 3 Contingency Training
- iv. NIST SP 800-53 Revision 4: CP 4 Contingency Plan Testing
- v. NIST SP 800-53 Revision 4: SA 14 Criticality Analysis

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

2. Disaster Recovery and Contingency Strategies

a. Disaster Recovery Plan (CP 2)

- i. DDSN shall develop a Disaster Recovery Plan (DRP) that addresses scope, roles, responsibilities, and coordination among organizational entities for reallocating information systems operations to an alternate location.
- ii. DDSN shall establish recovery time objectives for the BIA identified critical information systems.
- iii. DDSN shall establish and document procedures to fully restore critical information systems, post an incident, without deterioration of the security safeguards originally planned and implemented.
- iv. DDSN shall assign disaster recovery roles and responsibilities to key individuals.
- v. DDSN shall establish a process to ensure that the DRP is reviewed and approved by senior management.
- vi. DDSN shall distribute copies of the DRP to key personnel responsible for the recovery of the critical information systems and other relevant personnel and partners with contingency roles, as determined by the DDSN.
- vii. DDSN shall establish and implement procedures to review the DRP at planned intervals and at least on an annual basis.
- viii. DDSN shall establish a process to update the DRP when changes to the organization or environment of operation occurred.

b. Alternate Site (CP 7)

- i. DDSN shall identify and establish processes to relocate to an alternate site to facilitate the resumption of information system operations for business-critical functions within the defined recovery objectives (RTO and

Recovery Point Objective (RPO)) when the primary site is unavailable due to disruption.

- ii. DDSN shall ensure that equipment and supplies required to resume operations at the alternate processing site are available.
 - iii. DDSN shall ensure contracts are in place with third parties and suppliers to support delivery to the site within the defined time period for transfer/resumption of critical business operations.
 - iv. DDSN shall ensure that the alternate processing site provides information security safeguards similar to that of the primary site.
 - v. DDSN shall identify potential accessibility problems to the alternate site in the event of an area-wide disruption or disaster.
- c. Telecommunications Services (CP 8)
- i. DDSN shall establish primary and alternate telecommunication service agreements with priority-of-service provisions in accordance with organizational availability requirements (including RTOs), quality of service and access.
 - ii. DDSN shall establish alternate telecommunications services to facilitate the resumption of information system operations for critical business functions within the defined recovery objectives when the primary telecommunications capabilities are unavailable.
 - iii. DDSN shall require primary and alternate telecommunication service providers to have contingency plans.
 - iv. Information System Recovery and Reconstitution (CP 10).
 - v. DDSN shall establish documented procedures to restore and recover critical business activities from the temporary measures adopted to support normal business requirements after an incident.
 - vi. DDSN shall implement procedures for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.
 - vii. DDSN shall provide the capability to restore information system components within defined restoration time periods from configuration-controlled and integrity-protected information representing a known, operational state for the components (for e.g. reimaging methods).

- viii. DDSN shall establish measures to protect backup and restoration hardware, firmware, and software.
- d. Guidance:
 - i. NIST SP 800-53 Revision 4: CP 7 Alternate Processing Site
 - ii. NIST SP 800-53 Revision 4: CP 8 Telecommunications Services
 - iii. NIST SP 800-53 Revision 4: CP 10 Information System Recovery and Reconstitution

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

3. Data Backups

- a. Data Backup and Storage Policy
 - i. DDSN shall develop, maintain, and document a Data Backup and Storage Policy that address the adequate procedures to storage data and thus ensure the recovery of electronic information in the event of failure.
 - ii. DDSN shall identify and apply security requirements for protecting data backups based on the distinct types of data (sensitive, confidential, public) handle by the entity.
- b. Alternate Storage Site (CP 6)
 - i. DDSN shall identify an alternate storage site that is separated from the primary site so as not to be susceptible to same hazards to storage and recover information system backup information.
 - ii. DDSN shall establish necessary agreements with the site/location owner to ensure that data storage and retrieval process are not hindered during or post an incident.
 - iii. DDSN shall ensure that the alternate storage site provides information security safeguards similar to that of the primary storage site.
 - iv. DDSN shall identify potential accessibility problems to the alternate storage site in the event of a disruption or disaster.
 - v. DDSN shall identify secure transfer methods when transporting backup media off-site.
 - vi. DDSN shall establish and maintain an authorization list to retrieve backups from the off-site location.

- vii. DDSN shall review on an annual basis the security of the off-site location to ensure data is unexposed to unauthorized disclosure or modification while in storage.
- c. Information System Backup (CP 9)
- i. DDSN shall establish a process to perform data backups of user-level and system-level information at a defined frequency consistent with the established RTOs and RPOs.
 - ii. DDSN shall establish a process to perform data backups of information system security documentation at a defined frequency consistent with RTOs and RPOs.
 - iii. DDSN shall establish safeguards and controls to protect the confidentiality, integrity, and availability of backup information at storage locations.
 - iv. DDSN shall identify encryption/secure methods in storage of backup data to transportable media (i.e., tapes, CD Rooms, etc.).
 - v. DDSN shall enforce dual authorization (“two-person control”) for the deletion or destruction of DDSN sensitive data.
- d. Guidance:
- i. NIST SP 800-53 Revision 4: CP 6 Alternate Storage Site
 - ii. NIST SP 800-53 Revision 4: CP 9 Information System Backup

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

APPENDIX E

Human Resource and Security Awareness

1. Human Resource Compliance
 - a. Personnel Security Policy and Procedures (PE 1)
 - i. DDSN shall define security roles and responsibilities of employees, contractors and third-party users and shall be documented in accordance with DDSN information security policies.
 - b. Personnel Screening and Third-Party Personnel Security (PS 3) and (PS 7)
 - i. DDSN shall conduct background verification checks on all candidates for employment, including contractors, and third party users, which shall be carried out in accordance with relevant laws and DDSN Directive 406-04-DD: Criminal Record Checks and Reference Checks of Direct Caregivers.
 - c. Personnel Termination and Transfer (PS 4) and (PS 5)
 - i. Upon termination/transfer of employment for employees, termination of engagement for non-employees, or immediately upon request, personnel shall return to DDSN all agency documents (and all copies thereof) and other agency property and materials in their possession or control.
 - d. Access Agreements (PS 6)
 - i. As part of their information security obligation, employees, contractors and third party users shall agree and sign the Acceptable Use of Network Services and the Internet Form (DDSN Directive 367-09-DD), which shall state responsibilities for information security.
 - e. Guidance:
 - i. NIST SP 800-53 Revision 4: PE 1 Personnel Security Policy and Procedures
 - ii. NIST SP 800-53 Revision 4: PS 3 Personnel Screening
 - iii. NIST SP 800-53 Revision 4: PS 4 Personnel Termination
 - iv. NIST SP 800-53 Revision 4: PS 5 Personnel Transfer
 - v. NIST SP 800-53 Revision 4: PS 6 Access Agreements
 - vi. NIST SP 800-53 Revision 4: PS 7 Third-Party Personnel Security

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

2. Security Awareness Training

- a. Security Awareness Training and Information Security Workforce (AT 2) and (PM 13)
 - i. DDSN management shall require employees, contractors, and third-party users to apply security in accordance with established policies and procedures of the organization.
- b. Role-Based Security Training (AT 3)
 - i. DDSN shall impart appropriate awareness training and regular updates in organizational policies and procedures to all employees of the organization and to contractors and third-party users, as relevant for their job function.
 - ii. Training must be accompanied by an assessment procedure based on the cyber security training content presented to determine comprehension of key cyber security concepts and procedures.
 - iii. User access to DDSN information assets and systems will only be authorized for those users whose cyber security awareness training is current (e.g., having passed the most recent required training stage).
- c. Testing, Training, and Monitoring (PM 14)
 - i. DDSN will appoint a cyber-security awareness training coordinator to manage training content, schedules, and user training completion status.
 - ii. The DDSN cyber security training coordinator, along with the Information Security Officer will review training content on an annual basis to ensure that it aligns with State of South Carolina policies.
- d. Guidance:
 - i. NIST SP 800-53 Revision 4: AT 2 Security Awareness Training
 - ii. NIST SP 800-53 Revision 4: AT 3 Role-Based Security Training
 - iii. NIST SP 800-53 Revision 4: PM 13 Information Security Workforce
 - iv. NIST SP 800-53 Revision 4: PM 14 Testing, Training, and Monitoring

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

APPENDIX F

Information Security Information Systems Acquisitions, Development, and Maintenance

1. Change Management
 - a. Configuration Change Control (CM 3)
 - i. DDSN shall define change management controls to manage changes to information systems to minimize the likelihood of disruption, unauthorized alterations, and errors. The implementation of changes shall be controlled using a change control process. The following recommendations shall be followed for the change control process:
 1. All requests for change shall be managed in a structured way that determines the impact on the operational system and its functionality;
 2. All changes to production environments, including emergency maintenance and patches, shall be formally managed in a controlled manner;
 3. DDSN shall have a process to categorize, prioritize and authorize changes to information systems;
 4. Post-implementation reviews shall be performed to ensure production changes are operating as intended;
 5. A process shall be defined and communicated to ensure that all new modifications to the production environment have been adequately tested;
 6. A process for defining, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process shall be established; and
 7. Information systems shall be reviewed and tested after major changes to operating systems.
 - b. Guidance:
 - i. NIST SP 800-53 Revision 4: CM 3 Configuration Change Control

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>
2. Configuration Management
 - a. Policy Baseline Configuration (CM 2)
 - i. DDSN shall develop, review, and formally approve baseline configurations (most secure state) for critical information systems and infrastructure components.

- ii. DDSN shall develop a process to manage changes to baseline configurations, including identification, review, security impact analysis, test, and approval prior to implementation of changes.
 - iii. DDSN shall establish a central repository of all baseline configurations and shall implement access restrictions to prevent unauthorized changes.
 - iv. DDSN shall retain older versions of baseline configurations to be able to support rollback.
 - v. DDSN shall review and update baseline configurations periodically, and/or as an integral part of information system component installations or upgrades.
- b. Configuration Management Plan (CM 9)
- i. The DDSN shall assign responsibilities for developing and managing the configuration management process to personnel that are not directly involved in system development activities.
- c. Guidance
- i. NIST SP 800-53 Revision 4: CM 2 Baseline Configuration
 - ii. NIST SP 800-53 Revision 4: CM 9 Configuration Management Plan
 - iii. NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

3. System Development and Maintenance

- a. Policy System Security Plan (PL 2)
 - i. DDSN shall prepare system security plans and documentation for critical enterprise information systems or systems under development.
 - ii. System security plans shall provide an overview of the security requirements of the system and describe the controls in place for meeting the requirements through all stages of the systems development life cycle.
 - iii. When the system is modified in a manner that affects security, system documentation shall be updated accordingly.

- b. Vulnerability Scanning (RA 5)
 - i. DDSN shall perform a vulnerability assessment on all enterprise information systems undergoing significant changes before the systems are moved into production.
 - ii. DDSN shall perform periodic vulnerability assessments on production enterprise information systems and take appropriate measures to address the risks associated with any identified vulnerabilities.
 - iii. Vulnerability notifications from vendors and other appropriate sources shall be monitored and assessed for all information systems and applications.
- c. System and Services Acquisition Policy and Procedures (SA 2)
 - i. DDSN shall develop and follow a set of procedures consistent with State procurement standards as defined by the Division of Information Security and the Information Technology Management Office.
 - ii. DDSN shall ensure that the State's interests have been protected and enforced in all IT procurement contracts.
- d. System Development Life Cycle (SA 3)
 - i. DDSN shall implement appropriate security controls at all stages of the information system life cycle.
- e. External Information System Services (SA 9)
 - i. DDSN shall supervise and monitor outsourced software development to validate DDSN security requirements.
- f. Developer Security Testing and Evaluation (SA-11)
 - i. DDSN shall establish separate development, testing, and production environments.
 - ii. DDSN shall not use production data for testing purposes unless the data has been obfuscated, sanitized, or declassified. If production data must be temporarily used in these environments, appropriate security controls, including management approval, procedures to remove/delete data after completion of tests, and documentation of activities, shall be implemented.

- g. Flaw Remediation (SI 2)
 - i. DDSN shall design appropriate controls into information systems, including user developed applications to ensure correct processing.
 - ii. DDSN shall ensure that software patches are applied when they function to remove or reduce security weaknesses.
- h. Security Alerts, Advisories, and Directives (SI 5)
 - i. DDSN shall establish a process to collect information system security alerts, advisories, and directives on patches on an ongoing basis and implement these security directives in accordance with established time frames.
 - ii. A specific group or individual shall be given responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes.
- i. Software, Firmware, and Information Integrity (SI 7)
 - i. DDSN shall ensure that any decision to upgrade to a new release shall take into account the business requirements for the change, and the security of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version).
 - ii. DDSN shall test critical operating system (OS) changes and updates in the test environment to ensure there is no adverse impact on organizational operations or security.
- j. Information Input Validation (SI 10)
 - i. DDSN shall incorporate controls into information systems to check the validity of information inputs and information outputs.
 - ii. DDSN shall incorporate processing validation checks into information systems to detect processing errors, inadvertent or deliberate processing actions (e.g., accidental deletions).
- k. Session Authenticity (SC 23)
 - i. DDSN shall identify the appropriate controls to ensure session authenticity, protecting message integrity in applications and protecting information transmission to and from information systems.
- l. Policy Supplement
 - i. Threat and Vulnerability Management 1.1: Patch Management

- ii. Threat and Vulnerability Management 1.2: Vulnerability Assessment Solution

- m. Guidance:
 - i. NIST SP 800-53 Revision 4: PL 2 System Security Plan
 - ii. NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning
 - iii. NIST SP 800-53 Revision 4: SA 2 System and Services Acquisition Policy and Procedure
 - iv. NIST SP 800-53 Revision 4: SA 3 System Development Life Cycle
 - v. NIST SP 800-53 Revision 4: SA 9 External Information System Services
 - vi. NIST SP 800-53 Revision 4: SA 11 Developer Security Testing and Evaluation
 - vii. NIST SP 800-53 Revision 4: SI 2 Flaw Remediation
 - viii. NIST SP 800-53 Revision 4: SI 7 Software, Firmware, and Information Integrity
 - ix. NIST SP 800-53 Revision 4: SI 10 Information Input Validation
 - x. NIST SP 800-53 Revision 4: SC 23 Session Authenticity

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

4. Release Management

- a. Policy Allocation of Resources (SA 2)
 - i. DDSN shall ensure that production-ready release packages have been deployed using the release management lifecycle (i.e., plan, prepare, build, and test, pilot, and deploy).
 - ii. DDSN shall determine as part of the release planning process:
 - 1. Resources required to deploy the release;
 - 2. Pass/fail criteria;
 - 3. Build and test plans prior to implementation;
 - 4. Pilot and deployment plans; and
 - 5. Develop requirements for the release.

- b. Information System Documentation (SA 5)
 - i. DDSN shall document the set of tools and processes used to manage the IT release lifecycle, and the prioritization of the release.
 - ii. DDSN shall validate the release design against the requirements and identify the risks and potential issues.

- c. Security Engineering Principles (SA 8)
 - i. DDSN shall implement standardization and enforce operational controls using change requests for deploying releases into production.
- d. Guidance:
 - i. NIST SP 800-53 Revision 4: SA 2 Allocation of Resources
 - ii. NIST SP 800-53 Revision 4: SA 5 Information System Documentation
 - iii. NIST SP 800-53 Revision 4: SA 8 Security Engineering Principles

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

APPENDIX G

Information Security - IT Compliance

1. Audit and Compliance
 - a. Compliance with Legal and Contractual Requirements (A.15.1)
 - i. DDSN shall identify and document its obligations to applicable State, federal and other third-party laws, and regulations in relation to information security.
 - b. Compliance with Security Policies and Standards (A.15.2.1, A.15.2.2)
 - i. At least annually, DDSN shall perform reviews or audits of users' and systems' compliance with security policies, standards, and procedures, and initiate corrective actions where necessary.
 - ii. Results from compliance reviews or audits shall be documented and reported to DDSN leadership.
 - c. Audit and Accountability Policy and Procedures (AU 1)
 - i. DDSN shall establish a formal, documented audit and accountability policy and associated audit and accountability procedures.
 - ii. DDSN shall implement a process to review and update the audit and accountability policy and associated procedures at least annually.
 - d. Guidance:
 - i. ISO 27001:2005: A.15.1 Compliance with legal and contractual requirements
 - ii. ISO 27001:2005: A.15.2.1 Compliance with security policies and standards
 - iii. ISO 27001:2005: A.15.2.2 Technical compliance checking
 - iv. NIST SP 800-53 Revision 4
- To access any Guidance references, please see the attached link at:*
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>
2. Information System Audit Considerations
 - a. Information Systems Audit Controls (A.15.3.1)
 - i. DDSN shall implement audit procedures to help ensure that activities involving reviews or audits of operational systems are carefully planned to minimize the risk of disruptions to business processes.

- b. Protection of information systems audit tools (A.15.3.2)
 - i. DDSN shall implement security controls to help prevent unauthorized access and/or access abuse of audit tools.
- c. Audit Events (AU 2)
 - i. DDSN shall determine the type of events that are to be audited within information systems.
 - ii. DDSN shall review and update the list of audited events annually.
 - iii. DDSN leadership shall ensure coordination between the audit function, information security function, and business functions to facilitate the identification of auditable events.
- d. Content of Audit Records (AU 3)
 - i. DDSN information systems shall be enabled to generate audit records containing details to help establish what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of any individuals or subjects associated with the event.
- e. Audit Records Review and Reporting (AU 6)
 - i. DDSN shall analyze information system audit records periodically.
 - ii. DDSN shall report findings of audit records reviews to information security personnel and DDSN leadership.
 - iii. DDSN shall perform correlation and analysis of information generated by security assessments and monitoring.
- f. Audit Storage Capacity (AU 4)
 - i. DDSN shall allocate sufficient audit storage capacity to help ensure compliance with audit logs retention requirements from State, federal, and other applicable third-party laws, and regulations.
 - ii. DDSN shall implement provisions for information systems to off-load audit records at regular intervals onto a different system or media than the system being audited.
- g. Guidance:
 - i. ISO 27001:2005: A.15.3.1 Information systems audit controls

- ii. ISO 27001:2005: A.15.3.2 Protection of information systems audit tools
- iii. NIST SP 800-53 Revision 4: AU 2 Audit Events
- iv. NIST SP 800-53 Revision 4: AU 3 Content of Audit Records
- v. NIST SP 800-53 Revision 4: AU 4 Audit Storage Capacity
- vi. NIST SP 800-53 Revision 4: AU 6 Audit Review, Analysis, and Reporting

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

APPENDIX H

Information Security - IT Risk Strategy

I. Security Performance and Metrics

a. Information Security Measures of Performance (PM 6)

- i. DDSN shall develop, monitor, and report on performance metrics to demonstrate progress in adoption of security controls, and associated policies and procedures, and effectiveness of the information security program.
- ii. DDSN-defined performance measures should be able to support the determination of information system security posture, demonstrate compliance with requirements, and identify areas of improvement.

b. Manageability of Metrics (3.4.2)

- i. DDSN shall ensure that the metrics/ measures that are collected are meaningful, yield impact and outcome findings, and provide stakeholders with the time necessary to use the results to address performance gaps.

c. Data Management Concerns (3.4.3)

- i. DDSN shall standardize the data collection methods and data repositories used for metrics data collection and reporting to ascertain the validity and quality of data.

d. Guidance:

- i. NIST SP 800-53 Revision 4: PM 6 Information Security Measures of Performance
- ii. NIST SP 800-55 Revision 1: 3.4.2 Manageability
- iii. NIST SP 800-55 Revision 1: 3.4.3 Data Management Concerns

To access any Guidance references, please see the attached link at:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

2. Third Party Risk Management

a. External Information System Services (SA 9)

- i. DDSN shall establish a policy and associated processes to enforce that third parties comply with information security requirements and employ defined security controls in accordance with applicable federal laws,

Executive Orders, directives, policies, regulations, standards, and guidance.

- ii. DDSN shall implement processes, methods, and techniques to monitor security control compliance by third parties on an ongoing basis.
- b. Risk Assessment (RA 3)
 - i. DDSN shall establish a process to conduct risk assessments on third party service providers and document the risk assessment results.
 - ii. DDSN shall implement controls to help ensure that risk assessments are updated in case of major changes in scope of services or contractual changes with third parties.
- c. System Interconnections (CA 3)
 - i. DDSN shall authorize connections from DDSN information systems to third party information systems by entering into Interconnection Security Agreements.
 - ii. For each third-party interface, DDSN shall document the interface characteristics, security requirements, and the nature of the information communicated.
- d. Use of External Information Systems (AC 20)
 - i. DDSN shall establish terms and conditions for trust relationships established with other entities owning, operating, and/or maintaining external information systems.
 - ii. Terms and conditions established by DDSN should control:
 - 1. Access to DDSN information systems from third party information systems; and
 - 2. Controls for processing, storing, or transmit of DDSN data using third party information systems.
 - iii. DDSN shall review and update third party security agreements on an annual basis, or as defined in the contract.
- e. Information Sharing with Third Parties (UL 2)
 - i. DDSN shall share personally identifiable information (PII) with third parties only for the authorized purposes identified in the Privacy Act

and/or described in its notice(s), as well as State laws and Interconnection Security Agreements.

- ii. DDSN shall, where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the types of sensitive data covered (e.g., PII) and specifically enumerate the purposes for which the data may be used.
 - iii. DDSN shall monitor, audit, and train its staff on the authorized sharing of sensitive data with third parties and on the consequences of unauthorized use or sharing of such data.
 - iv. DDSN shall evaluate any proposed new instances of sharing sensitive data with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.
- f. Guidance:
- i. NIST SP 800-53 Revision 4: AC 20 Use of External Information Systems
 - ii. NIST SP 800-53 Revision 4: CA 3 System Interconnections
 - iii. NIST SP 800-53 Revision 4: PS 6 Access Agreements
 - iv. NIST SP 800-53 Revision 4: RA 3 Risk Assessment
 - v. NIST SP 800-53 Revision 4: SA 9 External Information System Services
 - vi. NIST SP 800-53 Revision 4: UL 2 Information Sharing with Third Parties

To access any Guidance references, please see the attached link at:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

APPENDIX I

Mobile Device Security

1. Security Procedures and Requirements
 - a. DDSN only allows access by mobile devices which are assigned and identified to an individual owner. Employees who are approved to access DDSN data or the DDSN data network using their personal device must register the device with the DDSN Information Technology Division (IT).
 - b. DDSN shall utilize mobile device management software to manage all mobile devices which access DDSN data or the DDSN data network. This includes agency owned and employee owned mobile devices.
 - c. DDSN shall utilize a mobile device management agent which will encrypt DDSN data on mobile devices using industry standard encryption techniques.
 - d. Employees must allow DDSN IT personnel to install DDSN's mobile device management agent to protect the security of DDSN data and the DDSN network.
 - e. Employees must allow DDSN IT personnel to scan mobile devices for viruses before they access DDSN data or the DDSN network. They must subsequently allow an automated virus scanning process to run on a regular basis without interfering with or aborting the process.
 - f. DDSN only allows access by mobile devices that can be remotely wiped / erased by DDSN's MDM software in the event of loss, theft, or evidence that DDSN data has been compromised.
 - g. Any mobile device must be approved by DDSN's designated Information Security Officer before accessing DDSN data or network. Only device types/operating systems that are supported by DDSN's MDM agent will be allowed to access DDSN's network and data.
 - h. Mobile devices with operating systems that have been modified from the standard provided by the mobile provider will not be allowed to access DDSN data or the DDSN network. "Rooting" and "Jail-breaking" is not allowed on phones which access DDSN data or the DDSN network.
 - i. Employees must notify DDSN's IT Division before the mobile device is disposed, sold, surrendered to a mobile provider, or otherwise deactivated and allow IT personnel to remove sensitive and confidential information from the mobile device.

- j. If a mobile device which has access to DDSN data or the DDSN network becomes lost or stolen, the employee must notify DDSN's IT Division immediately via the Helpdesk phone number or email. DDSN will maintain the technical capability of remotely wiping data from the lost or stolen device and will do so to mitigate risks associated with the lost or stolen mobile device.
 - k. All mobile devices which have access to DDSN data or the DDSN network must have security activated that requires a password or passcode to unlock the phone and gain access to its data. The timeout/lockout feature must be enabled which requires the password or passcode to be entered to gain access to the device after it has not been used for a period of time.
 - l. Unencrypted DDSN data shall not be copied to or stored on removable media on mobile devices (SD cards, etc.).
 - m. Unencrypted DDSN data shall not be copied from the mobile device to external storage media by any means (USB or other wired connectivity, Bluetooth, or other wireless technology).
2. Mobile Device Access Agreement
- a. Employees who are approved to have mobile devices which accesses DDSN data or the DDSN network shall sign the DDSN Mobile Device Access Agreement (see attachment) before being granted access.
 - b. The Mobile Device Access Agreement must also be signed by the manager of the employee requesting access. By doing so, the manager is indicating that the employee has a valid business need to access DDSN data and the DDSN network using a mobile device.
 - c. By signing the DDSN Mobile Device Access Agreement the employee agrees that the physical security of the device shall be the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out of-sight.

Mobile Device Access Agreement
South Carolina Department of Disabilities and Special Needs

1. EMPLOYEE

By signing below, I am requesting to use my personal mobile device to access DDSN data including, but not limited to, agency email. I agree to abide by the procedures and requirements of the DDSN Mobile Device Security Policy & DDSN Access Control Policy.

I understand that the policy includes, but is not limited to, the following:

- I agree that the physical security of the device is my responsibility and I will keep it in my physical possession whenever possible and store it in a secure place when it is not in my possession.
- I agree to notify the DDSN IT Division before the mobile device is disposed, sold, surrendered to a mobile provider, or otherwise deactivated and allow IT personnel to remove sensitive and confidential information from the mobile device.
- I agree to notify the DDSN IT Division immediately if my device becomes lost or stolen.
- I grant DDSN the right to install the DDSN mobile device management agent on my device.
- I grant DDSN the right to remotely wipe or erase data from my device should it be deemed necessary in order to protect the security and privacy of DDSN data. This may include loss of personal data stored on the device.
- I am aware that the use of this software is at my own risk, DDSN is not responsible for non-functioning or bricked devices, non-working SD cards, batteries or warranty void.

Print Employee Name

Signature

2. MANAGER

I certify that the above signed employee has a valid business need to access DDSN data using a mobile device.

Print Manager Name

Signature

Date: _____

Please return this form to: Kareem Briggs, Chief Information Security Officer by email at kareem.briggs@ddsn.sc.gov or by fax to (803) 898-9658

APPENDIX J

Physical Access and Environmental Security

1. Physical Security
 - a. Physical and Environmental Protection Policy and Procedures
 - i. DDSN shall establish formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
 - ii. DDSN shall establish procedures to review and maintain current the physical and environmental protection policy and associated procedures.
 - b. Physical Access Authorizations
 - i. DDSN shall develop, approve, and maintain a list of personnel with authorized access to the facility where information systems are physically located.
 - ii. DDSN shall establish a process to review, approve, and issue credentials for facility access.
 - iii. DDSN shall remove individuals from the facility access list when access is no longer required.
 - c. Physical Access Control
 - i. DDSN control entry to/exit from the data center(s) and/or sensitive facilities using physical access control devices (e.g., keycard or keys) and/or security guard(s).
 - ii. DDSN shall maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points.
 - iii. DDSN shall employ guards and/or alarms to monitor physical access points to the data center(s) where the information system resides 24 hours per day, 7 days per week.
 - iv. DDSN shall perform security assessments on an annual basis at the physical boundary of the data center(s) to check unauthorized exfiltration of information or removal of information system components.
 - v. DDSN shall establish a process to escort visitors and monitor their activity within the data center(s) and/or sensitive facilities.

- vi. DDSN shall change combinations and keys at defined intervals, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.
 - d. Access Control for Transmission Medium
 - i. DDSN shall control physical access to information system distribution and transmission lines within the data center(s) using physical access control devices (e.g., keycard or keys).
 - e. Access Control for Output Devices
 - i. DDSN shall place output devices in secured areas and in locations that can be monitored by authorized personnel and allow access to authorized individuals only.
 - ii. DDSN shall control physical access to information system output devices (e.g., printers, copiers, scanners, facsimile machines) to prevent unauthorized individuals from obtaining sensitive data.
 - f. Monitoring Physical Access
 - i. DDSN shall review physical access logs at a defined frequency and upon occurrence of security incidents.
 - g. Visitor Access Records
 - i. DDSN shall maintain visitor access records to the data center(s) and/or sensitive facilities for a minimum of one (1) year.
 - h. Delivery and Removal
 - i. DDSN shall establish processes to authorize, monitor, and control items entering and exiting the data center(s) and maintain records of those items.
- 2. Environmental Security
 - a. Policy Power Equipment and Cabling
 - i. DDSN shall place power equipment and cabling in safe locations to prevent environmental and/or man-made damage and destruction.
 - b. Emergency Shutoff
 - i. DDSN shall make available the capability of shutting off power to data center(s) during an incident.

- ii. DDSN shall place emergency shutoff switches or devices at locations which can be safely and easily accessed by personnel during an incident.
 - iii. DDSN shall implement physical and logical controls to protect emergency power shutoff capability from unauthorized activation.
 - c. Data Center Emergency Power
 - i. DDSN shall implement uninterruptible power supply to facilitate transition to long-term alternate power in the event of a primary power source loss.
 - d. Data Center Fire Protection
 - i. DDSN shall install and maintain fire detection and suppression devices that are supported by an independent power source.
 - ii. DDSN shall employ fire detection devices/system that activate automatically and notify emergency personnel and defined emergency responder(s) in the event of a fire.
 - iii. DDSN shall employ an automatic fire suppression system if/when the data center(s) is not staffed on a continuous basis.
 - e. Data Center Temperature and Humidity Controls
 - i. DDSN shall employ automatic temperature and humidity controls in the data center(s) to prevent fluctuations potentially harmful to processing equipment.
 - ii. DDSN shall employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.
 - f. Data Center Water Damage Protection
 - i. DDSN shall protect processing equipment from damage resulting from water leakage.
 - g. Guidance:
 - i. NIST SP 800-53 Revision 4: PE 1 Physical and Environmental Protection Policy and Procedures
 - ii. NIST SP 800-53 Revision 4: PE 2 Physical Access Authorizations
 - iii. NIST SP 800-53 Revision 4: PE 3 Physical Access Control

- iv. NIST SP 800-53 Revision 4: PE 4 Access Control for Transmission Medium
- v. NIST SP 800-53 Revision 4: PE 5 Access Control for Output Devices
- vi. NIST SP 800-53 Revision 4: PE 6 Monitoring Physical Access
- vii. NIST SP 800-53 Revision 4: PE 8 Visitor Access Records
- viii. NIST SP 800-53 Revision 4: PE 9 Power Equipment and Cabling
- ix. NIST SP 800-53 Revision 4: PE 10 Emergency Shutoff
- x. NIST SP 800-53 Revision 4: PE 11 Emergency Power
- xi. NIST SP 800-53 Revision 4: PE 13 Fire Protection
- xii. NIST SP 800-53 Revision 4: PE 14 Temperature and Humidity Controls
- xiii. NIST SP 800-53 Revision 4: PE 15 Water Damage Protection
- xiv. NIST SP 800-53 Revision 4: PE 16 Delivery and Removal

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

APPENDIX K

Information Security - Risk Management

1. Risk Management

- a. Risk management typically consists of the following:
 - i. Risk Assessment: A risk assessment is the first process of risk management and is used to determine the extent of the potential threat and the risk associated with IT security.
 - ii. Risk Mitigation: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls for the risks identified during the risk assessment process.
- b. Risk Management Strategy (PM 9)
 - i. DDSN shall define a schedule for an on-going risk assessment and risk mitigation process.
 - ii. DDSN shall review and evaluate risk based on the system categorization level and/or data classification of their systems.
- c. Guidance:
 - i. NIST SP 800-53 Revision 4: PM 9 Risk Management Strategy

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

2. Risk Assessment

- a. Policy Risk Assessment (RA 3)
 - i. The DDSN shall establish a risk assessment framework based on applicable State and federal laws, regulation, and industry standards. This assessment framework shall clearly define accountability, roles, and responsibilities.
- b. Security Assessment (CA 2)
 - i. DDSN shall annually conduct a formal assessment of the IT security processes and controls to determine the appropriateness of the design and implementation of controls, and the extent to which the controls are operating as intended and producing the desired outcome with respect to meeting the security requirements for their systems.

- ii. DDSN shall ensure that risk assessments identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the DDSN.
- c. Plan of Action and Milestones (CA 5)
 - i. DDSN shall develop and periodically update a Plan of Action and Milestones (POAM) document that shall identify any deficiencies related to internal security controls. The POAM shall identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during annual assessments.
 - ii. DDSN shall develop and periodically update a Corrective Action Plan (CAP) to identify activities planned or completed to correct deficiencies identified during the security assessment review. Both the POAM and the CAP shall address implementation of security controls to reduce or eliminate known risks in DDSN systems.
- d. Security Authorization (CA 6)
 - i. DDSN shall establish a process and assign a senior level executive or manager to determine whether or not risks can be accepted, and for each of the risks identified following the risk assessment, the designated personnel within the DDSN shall make a decision regarding risk treatment.
- e. Continuous Monitoring (CA 7)
 - i. DDSN shall continuously monitor the security controls within its information systems to ensure that the controls are operating as intended.
- f. Guidance:
 - i. NIST SP 800-15
 - ii. NIST SP 800-53 Revision 4: RA 3 Risk Assessment
 - iii. NIST SP 800-53 Revision 4: CA 2 Security Assessment
 - iv. NIST SP 800-53 Revision 4: CA 5 Plan of Action and Milestones
 - v. NIST SP 800-53 Revision 4: CA 6 Security Authorization
 - vi. NIST SP 800-53 Revision 4: CA 7 Continuous Monitoring

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

3. Risk Mitigation

- a. Continuous Monitoring (CA 7)
 - i. DDSN shall establish and implement controls to ensure risks are reduced to an acceptable level based on security requirements and once threats

have been identified and decisions for the management of risks have been made.

- ii. DDSN shall determine and document the acceptable level for risk for various threats based on the business requirements and the impact of the potential risk to the [Agency].

b. Guidance:

- i. NIST SP 800-53 Revision 4: CA 7 Continuous Monitoring

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

APPENDIX L

Information Security - Threat and Vulnerability Management

1. Vulnerability Assessment

a. Vulnerability Scanning (RA 5)

- i. DDSN shall implement processes to scan for vulnerabilities in information systems and hosted applications at least annually and when new vulnerabilities potentially affecting the information systems / applications are reported.
- ii. DDSN shall implement a process to control privileged access to vulnerability scanning tools and vulnerability reports.
- iii. DDSN shall analyze vulnerability scan reports and results from security control assessments.
- iv. DDSN shall remediate identified vulnerabilities in accordance with DDSN assessment of risk.

b. Penetration Testing (CA 8)

- i. DDSN shall conduct penetration testing exercises on an annual basis, either by use of internal resources or employing an independent third-party penetration team.

c. Guidance:

- i. NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning
- ii. NIST SP 800-53 Revision 4: CA 8 Penetration Testing

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

2. Incident Management

a. Incident Response Policy and Procedures (IR 1)

- i. DDSN shall develop, document, and publish an incident response policy that addresses scope, roles, and responsibilities, internal coordination efforts, and compliance.
- ii. DDSN shall establish formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

- iii. DDSN shall review and update the incident response policy and procedures on an annual basis.
- b. Incident Response Plan (IR 8)
 - i. DDSN shall develop and/or hire a third-party vendor to implement an incident response plan to:
 - 1. Establish a roadmap for implementing incident response capabilities;
 - 2. Identifies and documents the requirements of the organization, including mission, size, structure, and functions;
 - 3. Define the types of information security incidents to be reported;
 - 4. Establish metrics to help ensure incident response capabilities remain effective; and
 - 5. Define resources, such as technology and personnel, required to effectively support incident response capabilities.
 - ii. DDSN shall review and update the incident response plan on an annual basis.
- c. Incident Handling (IR 4)
 - i. DDSN shall implement formal processes to manage security incidents, including preparation, detection and analysis, containment, eradication, and recovery.
 - ii. DDSN shall implement dynamic response capabilities/tools such as intrusion detection, intrusion prevention systems, and firewalls, among others, to effectively respond to security incidents.
- d. Incident Monitoring and Reporting (IR 5, IR 6)
 - i. DDSN shall establish a process and tools to maintain detailed records of information security incidents that occur in external (e.g., boundary systems) and internal information systems.
 - ii. DDSN shall implement a policy to require personnel to report suspected information security incidents to the incident response team and/or DDSN leadership.
- e. Information System Monitoring (SI 4)
 - i. DDSN shall monitor information systems to detect attacks and/or signs of potential attacks, including unauthorized network local or remote connections.

- ii. DDSN shall deploy monitoring devices strategically within information technology environment to collect information security events and associated information.
 - iii. DDSN shall protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
 - iv. DDSN shall monitor inbound and outbound communications traffic to/from the information system for unusual or unauthorized activities or conditions.
 - v. DDSN shall heighten the level of information system monitoring activity whenever there is an indication of increased risk to DDSN operations, individuals, and assets,
- f. Incident Response Training (IR 2)
- i. DDSN shall provide incident response training within one (1) month of personnel assuming incident response roles or responsibilities.
 - ii. DDSN shall provide training to incident response personnel upon significant changes to information systems and/or changes to the incident response plan.
- g. Incident Response Testing (IR 3)
- i. DDSN shall establish a formal process to test incident response capabilities on a yearly basis to determine the incident response effectiveness and adequacy.
 - ii. DDSN shall document the incident response test results and update incident response processes as applicable.
- h. Malicious Code Protection (SI 3)
- i. DDSN shall employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
 - ii. DDSN shall implement a process to help ensure malicious code protection mechanisms are updated whenever new releases are available.
 - iii. DDSN shall configure malicious code protection mechanisms to perform periodic scans at defined time intervals.
 - iv. DDSN shall block malicious code and send an alert to information system/networks administrator and initiate action(s) in response to malicious code detection.

- i. Guidance
 - i. NIST SP 800-53 Revision 4: IR 1 Incident Response Policy and Procedures
 - ii. NIST SP 800-53 Revision 4: IR 2 Incident Response Training
 - iii. NIST SP 800-53 Revision 4: IR 3 Incident Response Testing
 - iv. NIST SP 800-53 Revision 4: IR 4 Incident Handling
 - v. NIST SP 800-53 Revision 4: IR 5 Incident Monitoring
 - vi. NIST SP 800-53 Revision 4: IR 6 Incident Reporting
 - vii. NIST SP 800-53 Revision 4: IR 8 Incident Response Plan
 - viii. NIST SP 800-53 Revision 4: SI 3 Malicious Code Protection
 - ix. NIST SP 800-53 Revision 4: SI 4 Information System Monitoring

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

3. Patch Management

- a. Flaw Remediation (SI 2)
 - i. DDSN shall develop and implement a process to identify, report, and correct information system flaws.
 - ii. DDSN shall establish a formal process to test software and firmware updates related to flaw remediation for effectiveness and identification of potential impact prior to implementation.
 - iii. DDSN shall install latest stable versions of applicable security software and firmware updates.
 - iv. DDSN shall establish a patch cycle that guides the normal application of patches and updates to systems.
 - v. DDSN shall establish a process of patch testing to verify the source and integrity of the patch and ensure testing in a production mirrored environment for a smooth and predictable patch roll out.
- b. Guidance:
 - i. NIST SP 800-53 Revision 4: SI 2 Flaw Remediation
 - ii. NIST SP 800-53 Revision 4: CM 2 Baseline Configuration

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

APPENDIX M

Data Protection and Privacy

1. Data Classification

a. Security Categorization (RA 2)

- i. DDSN shall categorize data in accordance with applicable federal and State laws, Executive Orders, directive, regulations, and information security guidance. DDSN data shall be classified into one of the following categories:
 1. **Public:** Information intended or required for sharing publicly. Examples of public information include information provided on government website, and reports meant for public distribution. Unauthorized disclosure, alteration or destruction of Public data would result in minimum to no risk to the State.
 2. **Internal Use:** Information that is used in daily operations of the DDSN. Examples of internal use information include DDSN hierarchy structure, internal procedures, and internal communications. Unauthorized disclosure, alteration or destruction of Internal Use data would result in negligible risk to the State.
 3. **Confidential:** Confidential information refers to sensitive information in custody of the DDSN. Examples of confidential information include credit card information, information security plan, system configuration standards, or information exempt from Freedom of Information Act (FOIA). Unauthorized disclosure, alteration or destruction of confidential data would result in considerable risk to the State.
 4. **Restricted:** Restricted information is highly sensitive information in custody or owned by the DDSN and/or data which is protected by Federal or State laws and regulations. Examples of restricted information may include, but are not limited to, Federal Tax Information (FTI) and health information protected by the Health Insurance Portability and Accountability Act (HIPAA). Unauthorized disclosure, alteration or destruction of restricted data shall result in considerable risk to the State including statutory penalties.
- ii. Users who encounter information that is improperly labeled, according to the data classification descriptions above, shall consult with the owner of the information and/or DDSN Information Security and/or Data Privacy team(s) to determine the appropriate data classification.

- iii. If multiple data fields with different classifications have been combined, the highest classification of information included shall determine the classification of the complete set.

b. Guidance

- i. NIST SP 800-53 Revision 4: RA 2 Security Categorization

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

2. Data Disposal

a. Policy Media Sanitization (MP 6)

- i. DDSN shall develop a list of approved processes for sanitizing electronic and non-electronic media prior to disposal, release for reuse and release outside of the DDSN based on applicable regulatory requirements.
- ii. DDSN shall employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
- iii. DDSN shall establish controls mechanism and processes for cleansing and disposal of computers, hard drives, and fax/printer/scanner devices.
- iv. DDSN shall implement controls to track media sanitization and disposal process, wherein such actions shall be tracked, documented, and verified.
- v. Media sanitization documentation shall provide a record of the media sanitized, when, how media was sanitized, the individual who performed the sanitization, and the final disposition of the media. The record of action taken shall be maintained in a written or electronic format.
- vi. DDSN shall test media sanitization equipment and procedures at least annually to ensure correct performance.
- vii. DDSN shall define and implement mechanisms for disposal of digital media and data storage devices contained in equipment to be redeployed outside of the DDSN.
- viii. Approved processes like physical destruction or digital degaussing shall be performed on devices, before they are disposed.
- ix. DDSN shall destroy hard copy media containing internal-use, confidential or restricted information using approved methods prior to disposal.

- x. The DDSN information security department shall monitor the destruction of hard copy media, as required to ensure and verify compliance with policy.

b. Guidance:

- i. NIST SP 800-53 Revision 4: MP 6 Media Sanitization

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

3. Data Protection

a. Policy System and Communications Protection Policy and Procedures (SC 1)

- i. The DDSN Information Security Officer and/or Data Privacy Officer shall be responsible for the development and implementation of policies and procedures to safeguard electronic protected, confidential, or restricted information.
- ii. DDSN employees shall follow DDSN's acceptable use policies when transmitting data.

b. Cryptographic Key Establishment and Management (SC 12)

- i. DDSN shall implement mechanisms to ensure availability of information in the event of the loss of cryptographic keys by users.
- ii. DDSN shall implement mechanisms to ensure the confidentiality of private keys.
- iii. DDSN shall develop a mechanism to randomly select a key from the entire key space, using hardware-based randomization.
- iv. DDSN shall implement appropriate controls to physically and logically safeguard the key-generating equipment from construction through receipt, installation, operation, and removal from service.

c. Cryptographic Protection (SC 17)

- i. For Restricted or data protected by Federal or State laws or regulations: DDSN shall use Federal Information Processing Standards (FIPS)-140 validated (e.g., Advanced Encryption Standards (AES), Triple Data Encryption Algorithm (TDEA), Diffie-Hellman, RSA, Rivest Cipher 5 (RC5)) technology for encrypting confidential data.

- ii. DDSN shall implement all encryption mechanisms to comply with this policy and support a minimum of, but not limited to the industry standard, AES 128-bit encryption.
- iii. DDSN shall not use any proprietary encryption algorithms for any purpose, unless approved by DDSN's information security department.
- d. Transmission Confidentiality and Integrity (SC 8 and SC 9)
 - i. Confidential or restricted information transmitted as an email message shall be encrypted based on DDSN encryption policy.
 - ii. Any confidential or restricted information transmitted through a public network to and from vendors, customers, or entities doing business with DDSN shall be encrypted or be transmitted through a tunnel encrypted by approved technologies such as virtual private networks (VPN), point-to-point tunnel protocols (PPTP) like secure socket layers (SSL).
 - iii. DDSN shall implement wireless encryption standards such as Wi-Fi Protected Access 2 (WPA2), and VPN encryption for remote wireless and/or internal network configurations to encrypt wireless transmissions that are used for transmitting confidential or restricted information.
 - iv. DDSN shall utilize encrypted file transfer programs such as "secured File Transfer Protocol (SFTP)" (FTP over Secure Shell (SSH) and Secure Copy (SCP) to secure transfer of documents and data over the Internet. Only authorized users shall be able to initiate secure transactions.
- e. Guidance:
 - i. NIST SP 800-53 Revision 4: SC 1 System and Communications Protection Policy and Procedures
 - ii. NIST SP 800-53 Revision 4: SC 8 Transmission Integrity
 - iii. NIST SP 800-53 Revision 9: SC 8 Transmission Confidentiality
 - iv. NIST SP 800-53 Revision 4: SC 12 Cryptographic Key Establishment and Management
 - v. NIST SP 800-53 Revision 4: SC17 Cryptographic Protection

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

4. Privacy

- a. Policy Privacy Impact Assessment
 - i. DDSN shall conduct a Privacy Impact Assessment (PIA) on information systems that will handle Personal Identifiable Information (PII).

- ii. DDSN shall publish privacy policies on DDSN websites used by the public.
 - iii. DDSN shall update PIAs when a system change creates new privacy risks (e.g., when functions applied to existing information collection change anonymous information into information in identifiable form).
 - iv. PIAs shall include:
 - 1. What information is to be collected (e.g., nature and source).
 - 2. Why information is being collected (e.g., to determine eligibility).
 - 3. Intended use of information (e.g., to verify existing data).
 - 4. With whom the information will be shared.
 - 5. What opportunities individuals have to decline to provide information.
 - 6. How the information will be secured.
 - v. The PIA document shall be reviewed by a DDSN executive or designee, such as CIO, CISO, or similar.
 - vi. DDSN shall provide a confidentiality agreement defining the responsibilities of the DDSN's employees and business partners (e.g., contractors, vendors) in maintaining the privacy of electronic information.
 - vii. The DDSN electronic information privacy officer, in conjunction with the DDSN human resources department, is responsible for the development and administration of this confidentiality agreement.
- b. Guidance:
- i. Fair Information Practice Principles (FIPPs)
 - ii. OMB Memorandum 03-22

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

APPENDIX N

Acceptable Use of Network Services and the Internet

1. General Principles

- a. Access to computer systems and networks owned or operated by DDSN and the State of South Carolina imposes certain responsibilities and obligations on state employees and officials (hereinafter termed “users”) and is subject to state government and DDSN policies and local, state and federal laws. Acceptable use always is ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual’s rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.
- b. Regardless of the physical location of the User’s workplace (e.g., telecommuting), the User is subject to the requirements of this directive.
- c. Users may be required to comply with supplemental requirements imposed for specific information systems.
- d. DDSN may inspect and/or seize any DDSN-issued device and/or data stored on any DDSN-issued information system and/or device. User acknowledges that he/she has no expectation of privacy as to any communication and/or information stored within any DDSN-issued information system or device, whether or not that information is stored locally, on a hard drive, or on other media in use with the unit.
- e. For network maintenance and security purposes, all DDSN information systems are subject to monitoring and interception of information. User acknowledges that DDSN may monitor and intercept User’s communications on DDSN information systems for purposes including, but not limited to, system testing, security, investigations of alleged personnel misconduct, and/or law enforcement investigations.
- f. Users who violate any copyright declarations are acting outside the course and scope of their employment with DDSN or other authority and the State of South Carolina is relieved of any legal responsibility. Users will be personally responsible and liable for such infringing activities.
- g. By participating in the use of networks and systems provided by DDSN and the State of South Carolina, users agree to be subject to and abide by this policy for their use. Willful violation of the principles and provisions of this policy may result in disciplinary action up to and including termination.

- h. In accordance with DDSN Directive 367-17-DD: Human Resource and Security Awareness Policy, employees, contractors, and third-party users shall agree and sign this policy.
 - i. User will complete DDSN privacy and security training prior to accessing any non-public data and/or DDSN information systems, and User will complete privacy and security training on an annual basis thereafter. User shall not take software home for personal use on a home computer.
 - j. This document may be updated on an as-needed basis and is subject to annual review.
2. Specific Provisions
- a. Users shall:
 - i. Agree that DDSN-issued devices and systems are the property of the DDSN and will be used only for DDSN authorized purposes, except that incidental use of DDSN resources/property is permitted as long as it does not result in additional public expense. Incidental use is infrequent and minimal. Unauthorized use of, or access to, a DDSN-issued device or systems is prohibited and may subject the user to employee discipline and/or legal actions.
 - ii. Refrain from monopolizing systems, overloading networks with excessive data or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.
 - iii. User will neither share his/her DDSN-issued User ID and/or password with any other person, nor knowingly allow any other person to use his/her User ID and/or password. If User suspects his/her password has been compromised, he/she will inform DDSN Information Technology Department and/or DDSN's Information Security Officer immediately.
 - iv. Assume personal responsibility for any charges associated with billable services unless appropriate authorization has been obtained.
 - v. At termination of employment, User will not remove from DDSN any information, hardware, software, device, or any other workplace resource, without explicit written permission from DDSN executive management; and
 - vi. At termination of employment, User will return all DDSN information, hardware, software, device, or any other workplace resource to User's supervisor.

- b. Users shall not:
- i. Use the DDSN-issued devices and systems for private purposes, including blogging, commenting or posting on social media, sharing photographs, or other non-work related purposes, without written permission from DDSN executive management including illegal, unlawful, immoral purposes or to support or assist such purposes. Examples of this would be the transmission of violent, threatening, defrauding, obscene or otherwise illegal or unlawful materials.

NOTE: It is advised that no DDSN business, consumer data or other DDSN-related information be shared to employees' personal social media pages. Please refer to DDSN Directive 413-04-DD: Social Media Usage, regarding how DDSN expects employees to use social media from a personal perspective.

- ii. Use mail or messaging services to harass, intimidate or otherwise annoy another individual.
- iii. Use the networks or other state equipment for private, recreational, non-public purposes including the conduct of personal commercial transactions.
- iv. Use the networks or other state equipment for commercial or partisan political purposes.
- v. Use the networks or other state equipment for personal gain such as selling access to a USER ID or by performing work for profit with state resources in a manner not authorized by the State.
- vi. Use the network to disrupt network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer "worms" and viruses, and sustained high volume network traffic which hinders others in their use of the network.
- vii. Attempt to circumvent or subvert system or network security measures.
- viii. Intercept network traffic for any purpose unless engaged in authorized network administrative duties.
- ix. Make or use illegal copies of copyrighted software or other mediums, store such copies on state systems, or transmit them over state networks.
- x. Store or back-up any DDSN non-public information to any non-DDSN information system or device such as portable hard drives

Acceptable Use of Network Services and the Internet
South Carolina Department of Disabilities and Special Needs

- I acknowledge that I have received a copy of the Acceptable Use of Network Services and the Internet policy.

- I acknowledge that I have read and understand the Acceptable Use of Network Services and the Internet policy.

- I authorize the Department of Disabilities and Special Needs (DDSN) staff to monitor any communications to or from myself on the DDSN network and internet.

- I understand that any violation of the provisions in the Acceptable Use of Network Services and the Internet policy is subject to the disciplinary action in accordance with DDSN's progressive disciplinary policy, and/or possible legal action.

- I agree to abide by DDSN's Acceptable Use of Network Services and the Internet policy.

User Name (Printed)

User Signature

Date: _____

APPENDIX O

Service Provider Data Protection

1. Purpose
 - a. Assure that each DSN Board/Provider assigns the responsibility for data security to a specific individual to provide organizational focus and importance to security, privacy and that the assignment of responsibility is documented.
 - b. Responsibilities include:
 - i. The management and supervision of the use of security measures to protect data, and
 - ii. The management and conduct of all personnel in relation to that data. This includes the notification of all additions, changes, or deletions of any user of DDSN information systems.
2. Statement
 - a. It is the policy of the South Carolina Department of Disabilities and Special Needs (DDSN) to have one official designated by each DSN Board/Provider as the Data Security Administrator who is responsible for the implementation of the required policies and procedures.
3. Standards
 - a. Assigned Security Responsibility – Policy Standards
 - i. Each DSN Board/Provider shall designate at least one (1) individual as the Data Security Administrator to coordinate data security and data privacy activities in conjunction with the DDSN Information Security Officer and/or Data Privacy Officer.
 1. The assignment of responsibility of the Data Security Administrator shall include the development and implementation of policies and procedures to safeguard electronic protected/confidential or restricted information within organizational requirements.
 2. The assignment of responsibility of the Data Security Administrator shall include the supervision over the conduct of all personnel in relation to the protection of electronic protected, confidential, or restricted information.
 3. The assignment and designation of the Data Security Administrator shall be documented.

- b. Assigned Security Responsibility - Procedural Standards
 - i. Each DSN Board/Provider shall have an individual designated for security responsibilities that will coordinate security activities locally.
 - ii. Each DSN Board/Provider's designated security administrator shall be responsible for ensuring all DDSN security procedures are followed by issuing and terminating DDSN security privileges.
 - iii. The Data Security Administrator shall be responsible for oversight of the conduct of personnel in the protection of the data locally at each DSN Board/Provider.

PROPOSED TO MARK OBSOLETE

Attachment J

Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration



3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/DSN-INFO
Website: www.ddsn.sc.gov

COMMISSION
William O. Danielson
Chairperson
Gary C. Lemel
Vice Chairman
Eva R. Ravenel
Secretary
Mary Ellen Barnwell
Sam F. Broughton, Ph.D.
Catherine O. Fayssoux
Vicki A. Thompson

Reference Number: 100-11-DD

Title of Document: Absence with Leave of District Director or Facility Administrator from Duty Station

Date of Issue: July 1, 1987
Effective Date: July 1, 1987
Last Review Date: July 11, 2016
Date of Last Revision: July 11, 2016 (NO REVISIONS)

Applicability: District Offices and Regional Centers

I. POLICY

The periodic absence of the District Directors or Facility Administrators from their duty stations is necessary to promote effective operations. Absence of the District Director or Facility Administrator must occur in accordance with pertinent department directives regarding leave and/or travel.

II. PROCEDURE

When the District Director or Facility Administrator is to be on leave from their duty station (to include annual, holiday or sick leave), the following notification procedures apply:

1. The District Director, for leave of one normal workday or more, must verbally notify the Associate State Director-Operations of the absence and the person designated to act in their absence, if necessary.

The Facility Administrator, for leave of one normal workday or more, must verbally notify the District Director of the absence and the person designated to act in their absence, if necessary.

DISTRICT I

P.O. Box 239
Clinton, SC 29325 5328
Phone: (864) 938 3497

Midlands Center -Phone: 803/935 7500
Whitten Center -Phone: 864/833 2733

DISTRICT II

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832 5576


Coastal Center -Phone: 843/873 5750
Pee Dee Center -Phone: 843/664 2600
Saleeby Center -Phone: 843/332 4104

2. The District Director, for anticipated leave longer than five consecutive normal work days, will provide written notice to the Associate State Director-Operations along with the designation of an Acting District Director to serve during the period of leave.

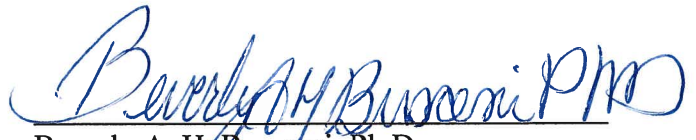
The Facility Administrator, for anticipated leave longer than five consecutive normal work days, will officially notify the office of the District Director along with the designation of an Acting Facility Administrator to serve during the period of leave. The District Director must in turn notify the Associate State Director-Operations of this absence.

The District Director or Facility Administrator will assure that key District Office or Regional Center staff will be notified of the designated Acting District Director or Acting Facility Administrator.

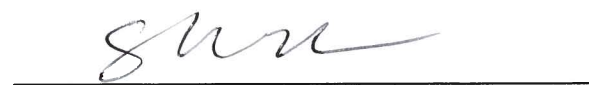
3. The Acting District Director and the Acting Facility Administrator shall be given instructions as to how the District Director or Facility Administrator can be reached in the event of an emergency regardless of their anticipated period of leave, and shall be given the name of an appropriate Central Office contact in the event reaching the District Director or Facility Administrator is impossible or impractical at the time of said emergency. The Central Office contact will normally be the Associate State Director-Operations. In the absence of this Associate State Director or unavailability, the contact is as follows: State Director, Associate State Director-Administration.



David A. Goodell
Associate State Director-Operations
(Originator)



Beverly A. H. Buscemi, Ph.D.
State Director
(Approved)



Susan Kreh Beck, Ed.S., NCSP
Associate State Director-Policy

PROPOSED TO MARK OBSOLETE

Attachment K

Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration



COMMISSION
William O. Danielson
Chairperson
Fred Lynn
Vice Chairman
Eva R. Ravenel
Secretary
Mary Ellen Barnwell
Katherine W. Davis
Gary C. Lemel
Vicki A. Thompson

3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/DSN-INFO
Website: www.ddsn.sc.gov

Reference Number: 367-09-DD

Title of Document: Acceptable Use of Network Services and the Internet

Date of Issue: July 3, 1996
Effective Date: July 3, 1996
Last Review Date: May 3, 2016
Date of Last Revision: May 3, 2016 (REVISED)

Applicability: DDSN Central Office, DDSN District Offices and DDSN Regional Centers

PURPOSE

This directive establishes the Agency's policy and guidelines regarding the use of the Department of Disabilities and Special Needs (DDSN) and other State of South Carolina computer networks and the internet.

General Principles

1. Access to computer systems and networks owned or operated by DDSN and the State of South Carolina imposes certain responsibilities and obligations on state employees and officials (hereinafter termed "users") and is subject to state government and DDSN policies and local, state and federal laws. Acceptable use always is ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual's rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.
2. Regardless of the physical location of the User's workplace (e.g., telecommuting), the User is subject to the requirements of this directive.

DISTRICT I

P.O. Box 239
Clinton, SC 29325-5328
Phone: (864) 938-3497

Midlands Center - Phone: 803/935-7500
Whitten Center - Phone: 864/833-2733

DISTRICT II

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832-5576

Coastal Center - Phone: 843/873-5750
Pee Dee Center - Phone: 843/664-2600
Saleeby Center - Phone: 843/332-4104

3. Users may be required to comply with supplemental requirements imposed for specific information systems;
4. DDSN may inspect and/or seize any DDSN-issued device and/or data stored on any DDSN-issued information system and/or device. User acknowledges that he/she has no expectation of privacy as to any communication and/or information stored within any DDSN-issued information system or device, whether or not that information is stored locally, on a hard drive, or on other media in use with the unit.
5. For network maintenance and security purposes, all DDSN information systems are subject to monitoring and interception of information. User acknowledges that DDSN may monitor and intercept User's communications on DDSN information systems for purposes including, but not limited to, system testing, security, investigations of alleged personnel misconduct, and/or law enforcement investigations.
6. Users who violate any copyright declarations are acting outside the course and scope of their employment with DDSN or other authority and the State of South Carolina is relieved of any legal responsibility. Users will be personally responsible and liable for such infringing activities.
7. By participating in the use of networks and systems provided by DDSN and the State of South Carolina, users agree to be subject to and abide by this policy for their use. Willful violation of the principles and provisions of this policy may result in disciplinary action up to and including termination.
8. In accordance with DDSN Directive 367-17-DD: Human Resource and Security Awareness Policy, employees, contractors and third party users shall agree and sign this policy.
9. User will complete DDSN privacy and security training prior to accessing any non-public data and/or DDSN information systems, and User will complete privacy and security training on an annual basis thereafter. User shall not take software home for personal use on a home computer.
10. This document may be updated on an as-needed basis and is subject to annual review.

Specific Provisions

Users shall:

1. Agree that DDSN-issued devices and systems are the property of the DDSN and will be used only for DDSN authorized purposes, except that incidental use of DDSN resources/property is permitted as long as it does not result in additional public expense. Incidental use is infrequent and minimal. Unauthorized use of, or access to, a DDSN-issued device or systems is strictly prohibited and may subject the user to employee discipline and/or legal actions;

2. Refrain from monopolizing systems, overloading networks with excessive data or wasting computer time, connect time, disk space, printer paper, manuals or other resources;
3. User will neither share his/her DDSN-issued User ID and/or password with any other person, nor knowingly allow any other person to use his/her User ID and/or password. If User suspects his/her password has been compromised, he/she will inform DDSN Information Technology Department and/or DDSN's Information Security Officer immediately;
4. Assume personal responsibility for any charges associated with billable services unless appropriate authorization has been obtained;
5. At termination of employment, User will not remove from DDSN any information, hardware, software, device, or any other workplace resource, without explicit written permission from DDSN executive management; and
6. At termination of employment, User will return any and all DDSN information, hardware, software, device, or any other workplace resource to User's supervisor.

Users shall not:

1. Use the DDSN-issued devices and systems for private purposes, including blogging, commenting or posting on social media, sharing photographs, or other non-work related purposes, without written permission from DDSN executive management including illegal, unlawful, immoral purposes or to support or assist such purposes. Examples of this would be the transmission of violent, threatening, defrauding, obscene or otherwise illegal or unlawful materials.
2. Use mail or messaging services to harass, intimidate or otherwise annoy another individual.
3. Use the networks or other state equipment for private, recreational, non-public purposes including the conduct of personal commercial transactions.
4. Use the networks or other state equipment for commercial or partisan political purposes.
5. Use the networks or other state equipment for personal gain such as selling access to a USER ID or by performing work for profit with state resources in a manner not authorized by the State.
6. Use the network to disrupt network users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer "worms" and viruses, and sustained high volume network traffic which substantially hinders others in their use of the network.
7. Attempt to circumvent or subvert system or network security measures.

8. Intercept network traffic for any purpose unless engaged in authorized network administrative duties.
9. Make or use illegal copies of copyrighted software or other mediums, store such copies on state systems, or transmit them over state networks.
10. Store or back-up any DDSN non-public information to any non-DDSN information system or device such as portable hard drives, USB drives or cloud service offerings in any form or format.



Tom Waring
Associate State Director-Administration
(Originator)



Beverly Buscemi, Ph.D.
State Director
(Approved)

ATTACHMENT: Acceptable Use of Network Services and the Internet

PROPOSED TO MARK OBSOLETE



Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration

COMMISSION
William O. Danielson
Chairperson
Fred Lynn
Vice Chairman
Eva R. Ravenel
Secretary
Mary Ellen Barnwell
Katherine W. Davis
Gary C. Lemel
Vicki A. Thompson

3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/DSN-INFO
Website: www.ddsn.sc.gov

Reference Number:

367-12-DD

Title of Document:

Service Provider Data Protection and Privacy Policy

Date of Issue:

June 30, 2009

Effective Date:

June 30, 2009

Last Review Date:

October 5, 2015

Date of Last Revision

October 5, 2015

(REVISED)

Applicability:

DSN Boards and Contract Service Providers

I. POLICY PURPOSE

The purpose of this policy is to assure that the responsibility for data security is assigned to a specific individual to provide organizational focus and importance to security, privacy and that the assignment is documented. Responsibilities include:

1. The management and supervision of the use of security measures to protect data, and
2. The management and conduct of all personnel in relation to that data. This includes the notification of all additions, changes or deletions of any user of DDSN information systems.

II. POLICY STATEMENT

It is the policy of the South Carolina Department of Disabilities and Special Needs (DDSN) to have one official designated by each DSN Board/Provider as the Data Security Administrator who is responsible for the implementation of the required policies and procedures.

DISTRICT I

P.O. Box 239
Clinton, SC 29325-5328
Phone: (864) 938-3497

Midlands Center - Phone: 803/935-7500
Whitten Center - Phone: 864/833-2733

DISTRICT II

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832-5576

Coastal Center - Phone: 843/873-5750
Pee Dee Center - Phone: 843/664-2600
Saleeby Center - Phone: 843/332-4104

III. POLICY AND PROCEDURAL STANDARDS

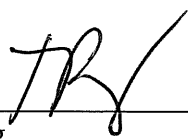
A. ASSIGNED SECURITY RESPONSIBILITY – POLICY STANDARDS

Each DSN Board/Provider shall designate at least one (1) individual as the Data Security Administrator to coordinate data security and data privacy activities in conjunction with the DDSN Information Security Officer and/or Data Privacy Officer.

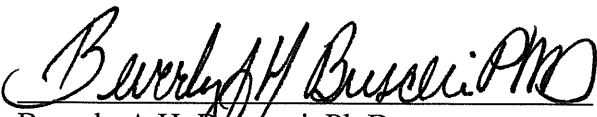
1. The assignment of responsibility of the Data Security Administrator shall include the development and implementation of policies and procedures to safeguard electronic protected/confidential or restricted information within organizational requirements.
2. The assignment of responsibility of the Data Security Administrator shall include the supervision over the conduct of all personnel in relation to the protection of electronic protected, confidential, or restricted information.
3. The assignment and designation of the Data Security Administrator shall be documented.

B. ASSIGNED SECURITY RESPONSIBILITY - PROCEDURAL STANDARDS

1. Each DSN Board/Provider shall have an individual designated for security responsibilities that will coordinate security activities locally.
2. Each DSN Board/Provider's designated security administrator shall be responsible for ensuring all DDSN security procedures are followed by issuing and terminating DDSN security privileges.
3. The Data Security Administrator shall be responsible for oversight of the conduct of personnel in the protection of the data locally at each DSN Board/Provider.



Tom Waring
Associate State Director-Administration
(Originator)



Beverly A.H. Buscemi, Ph.D
State Director
(Approved)

PROPOSED TO MARK OBSOLETE



Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration

COMMISSION
William O. Danielson
Chairman
Eva R. Ravenel
Vice Chairman
Gary C. Lemel
Secretary
Mary Ellen Barnwell
Sam F. Broughton, Ph.D.
Catherine O. Fayssox
Vicki A. Thompson

3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/DSN-INFO
Website: www.ddsn.sc.gov

Reference Number: 367-18-DD
Title of Document: Information Security Policy - Access Control
Date of Issue: October 5, 2015
Effective Date: October 5, 2015
Last Review Date: October 5, 2015
Date of Last Revision: July 13, 2016 (NEW)
Applicability: All DDSN Employees

I. ACCESS MANAGEMENT

The purpose of the access management section is to establish processes to control access and use of DDSN information resources. Access management incorporates role based access controls (RBAC), privileged user access, access definitions, roles, and profiles.

Access Control Policy and Procedures (AC 1)

DDSN shall establish formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Account Management (AC 2)

DDSN shall identify account types (e.g., individual, group, system, application, guest/anonymous, and temporary) and establish conditions for group membership.

DDSN shall identify authorized users of information systems and specify access rights.

Requests for access to DDSN Data must be approved by the business/data owner (or delegate) prior to provisioning the user account.

DISTRICT I

P.O. Box 239
Clinton, SC 29325-5328
Phone: (864) 938-3497

Midlands Center - Phone: 803/935-7500
Whitten Center - Phone: 864/833-2733

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832-5576

DISTRICT II

Coastal Center - Phone: 843/873-5750
Pee Dee Center - Phone: 843/664-2600
Saleeby Center - Phone: 843/332-4104

DDSN shall authorize and monitor the use of guest/anonymous and temporary accounts, and notify relevant personnel (e.g., account managers) when temporary accounts are no longer required.

DDSN shall utilize request for access change documentation (e.g., account managers, system administrators) to remove or deactivate access rights when users are terminated, transferred, or access rights requirements change.

DDSN shall remove or disable default user accounts and, if user accounts cannot be removed or disabled, they should be renamed.

Access shall be granted based upon the principles of need-to-know, least-privilege, and separation of duties. Access not explicitly permitted shall be denied by default.

Access requests from users shall be recorded and follow the DDSN established approval process.

DDSN shall ensure that user access requests are approved by a business owner (or any other pre-approved role).

Privileged accounts (e.g., system/network administrators having root level access, database administrators), shall only be allowed after approval by a DDSN information security officer and/or similarly designated role. The approval shall be granted to a limited number of individuals with the requisite skill, experience, business need, and documented reason based on role requirements.

DDSN shall ensure that privileged accounts are controlled, monitored, and can be reported on a periodic basis.

DDSN shall enforce periodic user access reviews to be performed by information/data owners or their assigned delegate(s) to ensure the following:

- Access levels remain appropriate, based upon approvals;
- Terminated employees do not have active accounts;
- There are no group accounts, unless approved; and
- There are no duplicate user identifiers.

DDSN shall review information system accounts within every 180 days and require annual certification.

DDSN shall regulate information system access and define security requirements for contractors, vendors, and other service providers.

DDSN shall administer privileged user accounts in accordance with a role-based access model.

Access Enforcement (AC 3)

DDSN shall enforce approved authorizations for logical access to information systems.

DDSN shall implement encryption as an access control mechanism if required by Federal, State or other laws or regulations.

Information Flow Enforcement (AC 4)

For Restricted data: DDSN systems shall enforce data flow controls using security attributes on information, source, and destination objects as a basis for flow control decisions.

Separation of Duties (AC 5)

DDSN shall implement controls in information systems to enforce separation of duties through assigned access authorizations, including but not limited to:

- Audit functions are not performed by security personnel responsible for administering information system access;
- Divide critical business and information system management responsibilities;
- Divide information system testing and production functions between different individuals or groups; and
- Independent entity to conduct information security testing of information systems.

DDSN shall document and implement separation of duties through assigned information system access authorizations.

Least Privilege (AC 6)

DDSN shall ensure that only authorized individuals have access to DDSN data/information and that such access is strictly controlled, audited in accordance with the concepts of “need-to-know, least-privilege, and separation of duties.”

DDSN shall implement processes or mechanisms to:

- Disable file system access not explicitly required for system, application, and administrator responsibilities;
- Provide minimal physical and system access to the contractors and ensure information security policy adherence by all contractors;
- Restrict use of database management to authorized database administrators;

- Grant access to authorized users based on their required job duties; and
- Disable all system and removable media boot access unless explicitly authorized by the CIO; if authorized, boot access shall be password protected.

Unsuccessful Login Attempts (AC 7)

DDSN systems shall enforce a limit of unsuccessful logon attempts during a DDSN-defined period. The number of logon attempts shall be commensurate with the classification of data hosted, processed or transferred by the information system.

DDSN shall automatically lock user accounts the after maximum logon attempts is reached. DDSN shall establish an account lock time period commensurate with the classification of data hosted, processed or transferred by the information system.

System Use Notification (AC 8)

DDSN systems shall display the following warning before granting system access. “This system is solely for the use of authorized DDSN personnel. The information contained herein is the property of DDSN and subject to non-disclosure, security and confidentiality requirements. DDSN shall monitor system usage for unauthorized activities. Any user accessing this system expressly consents to such monitoring.”

Session Lock (AC 11)

DDSN systems shall time out sessions or require a re-authentication process after 30 minutes or less of inactivity.

Guidance: *NIST SP 800-53 Revision 4: AC 1 Access Control Policy And Procedures*
 NIST SP 800-53 Revision 4: AC 3 Access Enforcement
 NIST SP 800-53 Revision 4: AC 4 Information Flow Enforcement
 NIST SP 800-53 Revision 4: AC 5 Separation Of Duties
 NIST SP 800-53 Revision 4: AC-6 Least Privilege
 NIST SP 800-53 Revision 4: AC 7 Unsuccessful Login Attempts
 NIST SP 800-53 Revision 4: AC 8 System Use Notification
 NIST SP 800-53 Revision 4: AC 11 Session Lock

NETWORK ACCESS MANAGEMENT

The purpose of the network access management section is to establish procedures to control and monitor access and use of the network infrastructure. These are necessary to preserve the integrity, availability and confidentiality of DDSN information. Users of these services are therefore advised of this potential monitoring and agree to this practice.

Remote Access (AC 17)

DDSN shall document allowed methods for remote access to the network and information systems.

DDSN shall utilize automated mechanisms to enable management to monitor and control remote connections into networks and information systems.

Virtual Private Network (VPN) or equivalent encryption technology shall be used to establish remote connections with DDSN networks and information systems.

Remote users shall connect to DDSN information systems only using mechanism protocols approved by the DDSN through a limited number of managed access control points for remote connections.

For Restricted data and/or system administrators: DDSN employees and authorized third parties accessing DDSN information systems remotely shall do so via an approved two-factor authentication (2FA) technology.

DDSN shall develop formal procedures for authorized individuals to access its information systems from external systems, such as access allowed from an alternate work site (if required).

Wireless Access (AC 18)

DDSN establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

DDSN shall only use wireless networking technology that enforces user authentication.

DDSN shall authorize wireless access to information systems prior to allowing use of wireless networks.

DDSN does not allow wireless access points to be installed independently by users.

Use of External Information Systems (AC 20)

If external systems are authorized by the DDSN, the DDSN shall establish terms and conditions for their use, including types of applications that can be accessed from external information systems, security category of information that can be processed, stored, and transmitted, use of VPN and firewall technologies, the use and protection against the vulnerabilities of wireless technologies, physical security maintenance and the security capabilities of installed software are to be updated.

Boundary Protection (SC 7)

DDSN networks where information deemed critical by DDSN is stored or processed shall be physically or logically segregated from publicly available networks.

DDSN networks and information systems shall not be accessible from public networks (e.g., Internet) except under secured and managed interfaces employing boundary protection devices.

DDSN limits network access points to a minimum to enable effective monitoring of inbound and outbound communications and network traffic.

Guidance: *NIST SP 800-53 Revision 4: AC 17 Remote Access*
 NIST SP 800-53 Revision 4: AC 18 Wireless Access
 NIST SP 800-53 Revision 4: AC 20 Use of External Information Systems
 NIST SP 800-53 Revision 4: SC 7 Boundary Protection

IDENTITY MANAGEMENT

The purpose of the identity management section is to establish a standardized method to create and maintain verifiable user identifiers, and enable decisions about the levels of access to be given to each individual and/or groups.

Identification and Authentication (IA 2, IA 4 AND IA 8)

DDSN shall establish processes to enforce the use of unique system identifiers (User IDs) assigned to each user, including technical support personnel, system operators, network administrators, system programmers, and database administrators.

DDSN shall prevent reuse of user identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier.

DDSN shall allow the use of group IDs only where these are necessary for business or operational reasons; group IDs shall be formally approved and documented.

If DDSN requires group IDs, it shall require individuals to be authenticated with a unique user account prior to using the group ID (e.g., network authentication prior to use of Group ID).

DDSN shall minimize the use of system, application, or service accounts; and DDSN shall document, formally approve, and designate a responsible party of this type of accounts.

DDSN security system shall be able to identify and verify the identification and, if deemed necessary by DDSN, the location of each authorized user.

Guidance: *NIST SP 800-53 Revision 4: IA 2 Identification and Authentication (Organizational Users)*
 NIST SP 800-53 Revision 4: IA 4 Identifier Management
 NIST SP 800-53 Revision 4: IA 8 Identification and Authentication (Non-Organizational Users)

AUTHENTICATION

The purpose of the authentication section is to establish the authentication methods utilized by the DDSN for authenticating, external/remote access connections, VPN access, administrative function access, vendor access and remote access to sensitive information.

Authenticator Management (IA 5)

DDSN shall choose a suitable multifactor authentication technique to substantiate the claimed identity of a user.

Unsuccessful Logon Attempts (AC 7)

DDSN shall implement mechanisms to record successful and failed authentication attempts.

Session Lock (AC 11)

DDSN shall define a maximum number of invalid logon attempts commensurate to the criticality of network or information systems.

DDSN networks and information systems shall disable user access upon reaching the maximum number of invalid access attempts as defined by the DDSN.

Network and information systems sessions should remain locked for a predetermined time or until the user reestablishes access through an established authentication procedure.

Guidance: NIST SP 800-53 Revision 4: AC 7 Unsuccessful Logon Attempts
NIST SP 800-53 Revision 4: AC 11 Session Lock
NIST SP 800-53 Revision 4: IA 5 Authenticator Management

EMERGENCY ACCESS

The purpose of the emergency access section is to establish conditions under which emergency access is granted, outlines rules to determine who is eligible to obtain emergency access and the authorized personnel entitled to grant access.

Policy Account Management (AC 2)

DDSN shall establish processes and procedures for users to obtain access to required information systems on an emergency basis.

The emergency procedures shall ensure that:

- Only identified and authorized personnel are allowed access to live systems and data;
- All emergency actions are documented in detail; and
- Emergency action is reported to management and reviewed in an orderly manner.

DDSN will establish a process to automatically terminate emergency accounts within 24 hours and temporary accounts with a fixed duration not to exceed 365 days.

Guidance: NIST SP 800-53 Revision 4: AC 2 Account Management

PASSWORD POLICY

The purpose of the password policy section is to establish uniform and enterprise-wide practices to create, manage and maintain passwords to ensure expected level of access security. The policy outlines requirements for creation of strong passwords, protection of those passwords, and password change frequency.

Account Management (AC 2)

DDSN shall establish a process for password-based authentication to include the following:

- Automatically force users (including administrators) to change user account passwords every 90 days.
- Automatically force system administrators (including database, network, and application administrators) to change user account passwords no less than every 60 days;
- Passwords for system accounts to be changed at least every one hundred 180 days;
- Enforce password minimum lifetime of one (1) day;
- Prohibit the use of dictionary names or words as passwords;
- Enforce password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lowercase letters, and numbers) and/or special characters;
- Enforce a minimum number of characters to be changed when new passwords are created. For Restricted data consider a minimum of four (4) changed characters.
- Encrypt passwords in storage and during transmission;
- Prohibit password reuse for six (6) generations prior to reuse;

DDSN users shall not share passwords with others under any circumstance.

System passwords shall be changed immediately upon termination / resignation of any employee with privileged access.

DDSN shall not allow users to use common words or based on personal information as passwords (e.g., username, social security number, children's names, pets' names, hobbies, anniversary dates, etc.).

DDSN shall suspend user accounts after a specified number of days of inactivity.

DDSN shall implement a process to change passwords immediately if there reason to believe a password has been compromised or disclosed to someone other than the authorized user.

Guidance: NIST SP 800-53 Revision 4: AC 2 Account Management

PASSWORD ADMINISTRATION

The purpose of the password administration section is to ensure that the allocation of passwords is controlled through a formal management process.

Policy Access Agreements (PS 6)

DDSN users shall sign an acknowledgement to evidence understanding of authentication policies, including the DDSN policy to keep passwords confidential and to keep group passwords solely within the members of the group.

DDSN shall require that employees sign acknowledgement prior to allowing access to network and information systems.

Identification and Authentication (IA 2, IA 6 and IA 8)

DDSN shall establish a process to verify the identity of a user prior to providing a new, replacement or temporary password.

DDSN shall establish a process to uniquely identify and authenticates non-Agency users.

DDSN shall establish procedures to manage new or removed privileged accounts passwords.

Authenticator Management (IA 5)

First-time passwords shall be set to a unique value per user and changed immediately after first use.

DDSN shall provide temporary passwords to users in a secure manner; the use of third parties or unprotected (i.e., clear text) electronic mail messages shall be prohibited.

DDSN shall not allow default passwords for network and remote applications.

Authenticator Feedback (IA 6)

DDSN shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

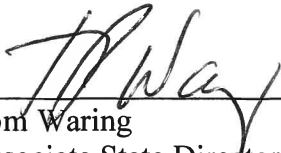
Guidance: *NIST SP 800-53 Revision 4: IA 2 Identification and Authentication (Organizational Users)*
 NIST SP 800-53 Revision 4: IA 5 Authenticator Management
 NIST SP 800-53 Revision 4: IA 6 Authenticator Feedback
 NIST SP 800-53 Revision 4: IA 8 Identification and Authentication (Non-Organizational Users)
 NIST SP 800-53 Revision 4: PS 6 Access Agreements

IMPLEMENTATION, MAINTENANCE, AND COMPLIANCE

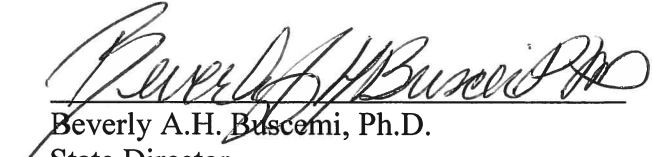
DDSN's designated Information Security Officer is responsible for insuring that this policy is implemented and communicated throughout the DDSN.

Any revisions to this policy shall be developed by the Information Security Officer and follow the normal approval process for DDSN directives.

Violation of the provisions of this policy will be subject to disciplinary action in accordance with DDSN's progressive discipline policy.



Tom Waring
Associate State Director-Administration
(Originator)



Beverly A.H. Buscemi, Ph.D.
State Director
(Approved)

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

PROPOSED TO MARK OBSOLETE



Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration

COMMISSION
William O. Danielson
Chairman
Eva R. Ravenel
Vice Chairman
Gary C. Lemel
Secretary
Mary Ellen Barnwell
Sam F. Broughton, Ph.D.
Catherine O. Fayssoix
Vicki A. Thompson

3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/DDS-INFO
Website: www.dds.sc.gov

Reference Number: 367-19-DD
Title of Document: Physical Access and Environmental Security Policy
Date of Issue: July 13, 2015
Effective Date: July 13, 2015
Last Review Date: July 13, 2015
Date of Last Revision: July 13, 2016 (NEW)
Applicability: All DDSN Employees

I. PURPOSE

The purpose of the Physical Access and Security section is to establish controls to prevent unauthorized physical access to DDSN information assets to protect them from damage, interruption, misuse, destruction and/or theft.

II. PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

- DDSN shall establish formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
- DDSN shall establish procedures to review and maintain current the physical and environmental protection policy and associated procedures.

Physical Access Authorizations

- DDSN shall develop, approve, and maintain a list of personnel with authorized access to the facility where information systems are physically located.

DISTRIC I

P.O. Box 239
Clinton, SC 29325-5328
Phone: (864) 938-3497

Midlands Center - Phone: 803/935-7500
Whitten Center - Phone: 864/833-2733

DISTRIC II

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832-5576

Coastal Center - Phone: 843/873-5750
Pee Dee Center - Phone: 843/664-2600
Saleeby Center - Phone: 843/332-4104

- DDSN shall establish a process to review, approve, and issue credentials for facility access.
- DDSN shall remove individuals from the facility access list when access is no longer required.

Physical Access Control

- DDSN control entry to/exit from the data center(s) and/or sensitive facilities using physical access control devices (e.g., keycard or keys) and/ or security guard(s).
- DDSN shall maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points.
- DDSN shall employ guards and/or alarms to monitor physical access points to the data center(s) where the information system resides 24 hours per day, 7 days per week.
- DDSN shall perform security assessments on an annual basis at the physical boundary of the data center(s) to check unauthorized exfiltration of information or removal of information system components.
- DDSN shall establish a process to escort visitors and monitor their activity within the data center(s) and/or sensitive facilities.
- DDSN shall change combinations and keys at defined intervals, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Access Control for Transmission Medium

- DDSN shall control physical access to information system distribution and transmission lines within the data center(s) using physical access control devices (e.g., keycard or keys).

Access Control for Output Devices

- DDSN shall place output devices in secured areas and in locations that can be monitored by authorized personnel, and allow access to authorized individuals only.
- DDSN shall control physical access to information system output devices (e.g., printers, copiers, scanners, facsimile machines) to prevent unauthorized individuals from obtaining sensitive data.

Monitoring Physical Access

- DDSN shall review physical access logs at a defined frequency and upon occurrence of security incidents.

Visitor Access Records

- DDSN shall maintain visitor access records to the data center(s) and/or sensitive facilities for a minimum of one (1) year.

Delivery and Removal

- DDSN shall establish processes to authorize, monitor, and control items entering and exiting the data center(s) and maintain records of those items.

III. ENVIRONMENTAL SECURITY

The purpose of the Environmental Security section is to define controls to protect DDSN information assets from damage, destruction and/or interruption due to environmental factors such as fire, humidity, water, power outage, etc.

Policy Power Equipment and Cabling

- DDSN shall place power equipment and cabling in safe locations to prevent environmental and/or man-made damage and destruction.

Emergency Shutoff

- DDSN shall make available the capability of shutting off power to data center(s) during an incident.
- DDSN shall place emergency shutoff switches or devices at locations which can be safely and easily accessed by personnel during an incident.
- DDSN shall implement physical and logical controls to protect emergency power shutoff capability from unauthorized activation.

Data Center Emergency Power

- DDSN shall implement uninterruptible power supply to facilitate transition to long-term alternate power in the event of a primary power source loss.

Data Center Fire Protection


- DDSN shall install and maintain fire detection and suppression devices that are supported by an independent power source.
- DDSN shall employ fire detection devices/system that activate automatically and notify emergency personnel and defined emergency responder(s) in the event of a fire.
- DDSN shall employ an automatic fire suppression system if/when the data center(s) is not staffed on a continuous basis.

Data Center Temperature and Humidity Controls


- DDSN shall employ automatic temperature and humidity controls in the data center(s) to prevent fluctuations potentially harmful to processing equipment.
- DDSN shall employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

Data Center Water Damage Protection

- DDSN shall protect processing equipment from damage resulting from water leakage.



Tom Waring
Associate State Director-Administration
(Originator)



Beverly A.H. Buscemi, Ph.D.
State Director
(Approved)

*Reference: NIST SP 800-53 Revision 4: PE 1 Physical and Environmental Protection Policy and Procedures
NIST SP 800-53 Revision 4: PE 2 Physical Access Authorizations
NIST SP 800-53 Revision 4: PE 3 Physical Access Control
NIST SP 800-53 Revision 4: PE 4 Access Control for Transmission Medium
NIST SP 800-53 Revision 4: PE 5 Access Control for Output Devices
NIST SP 800-53 Revision 4: PE 6 Monitoring Physical Access
NIST SP 800-53 Revision 4: PE 8 Visitor Access Records
NIST SP 800-53 Revision 4: PE 9 Power Equipment and Cabling
NIST SP 800-53 Revision 4: PE 10 Emergency Shutoff
NIST SP 800-53 Revision 4: PE 11 Emergency Power
NIST SP 800-53 Revision 4: PE 13 Fire Protection
NIST SP 800-53 Revision 4: PE 14 Temperature and Humidity Controls
NIST SP 800-53 Revision 4: PE 15 Water Damage Protection
NIST SP 800-53 Revision 4: PE 16 Delivery and Removal*

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

PROPOSED TO MARK OBSOLETE

Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration



3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/LSN-INFO
Website: www.ddsn.sc.gov

COMMISSION
William O. Danielson
Chairman
Eva R. Ravenel
Vice Chairman
Gary C. Lemel
Secretary
Mary Ellen Barnwell
Sam F. Broughton, Ph.D.
Catherine O. Faysoux
Vicki A. Thompson

Reference Number: 367-21-DD
Title of Document: Data Protection and Privacy Policy
Date of Issue: October 5, 2015
Effective Date: October 5, 2015
Last Review Date: October 5, 2015
Date of Last Revision: July 13, 2016 (NEW)
Applicability: All DDSN Employees

DATA CLASSIFICATION

The purpose of the data classification section is to define the different categories for DDSN information assets regardless of form whether it is electronic, hard copy, or intellectual property.

Security Categorization (RA 2)

DDSN shall categorize data in accordance with applicable federal and State laws, Executive Orders, directive, regulations, and information security guidance. DDSN data shall be classified into one of the following categories:

1. Public

Information intended or required for sharing publicly. Examples of public information include information provided on government website, and reports meant for public distribution. Unauthorized disclosure, alteration or destruction of Public data would result in minimum to no risk to the State.

DISRICT I

DISRICT II

2. Internal Use

Information that is used in daily operations of the DDSN. Examples of internal use information include DDSN hierarchy structure, internal procedures, and internal communications. Unauthorized disclosure, alteration or destruction of Internal Use data would result in little risk to the State.

3. Confidential

Confidential information refers to sensitive information in custody of the DDSN. Examples of confidential information include credit card information, information security plan, system configuration standards, or information exempt from Freedom of Information Act (FOIA). Unauthorized disclosure, alteration or destruction of confidential data would result in considerable risk to the State.

4. Restricted

Restricted information is highly sensitive information in custody or owned by the DDSN and/or data which is protected by Federal or State laws and regulations. Examples of restricted information may include, but are not limited to, Federal Tax Information (FTI) and health information protected by the Health Insurance Portability and Accountability Act (HIPAA). Unauthorized disclosure, alteration or destruction of restricted data shall result in considerable risk to the State including statutory penalties.

Users who encounter information that is improperly labeled, according to the data classification descriptions above, shall consult with the owner of the information and/or DDSN Information Security and/or Data Privacy team(s) to determine the appropriate data classification.

If multiple data fields with different classifications have been combined, the highest classification of information included shall determine the classification of the entire set.

Guidance NIST SP 800-53 Revision 4: RA 2 Security Categorization

DATA DISPOSAL

Policy Media Sanitization (MP 6)

DDSN shall develop a list of approved processes for sanitizing electronic and non-electronic media prior to disposal, release for reuse and release outside of the DDSN based on applicable regulatory requirements.

DDSN shall employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

DDSN shall establish controls mechanism and processes for cleansing and disposal of computers, hard drives, and fax/printer/scanner devices.

DDSN shall implement controls to track media sanitization and disposal process, wherein such actions shall be tracked, documented, and verified.

Media sanitization documentation shall provide a record of the media sanitized, when, how media was sanitized, the individual who performed the sanitization, and the final disposition of the media. The record of action taken shall be maintained in a written or electronic format.

DDSN shall test media sanitization equipment and procedures at least annually to ensure correct performance.

DDSN shall define and implement mechanisms for disposal of digital media and data storage devices contained in equipment to be redeployed outside of the DDSN.

Approved processes like physical destruction or digital degaussing shall be performed on devices, before they are disposed.

DDSN shall destroy hard copy media containing internal-use, confidential or restricted information using approved methods prior to disposal.

The DDSN information security department shall monitor the destruction of hard copy media, as required to ensure and verify compliance with policy.

Guidance NIST SP 800-53 Revision 4: MP 6 Media Sanitization

DATA PROTECTION

Policy System and Communications Protection Policy and Procedures (SC 1)

The DDSN Information Security Officer and/or Data Privacy Officer shall be responsible for the development and implementation of policies and procedures to safeguard electronic protected, confidential, or restricted information.

DDSN employees shall follow DDSN's acceptable use policies when transmitting data.

Cryptographic Key Establishment and Management (SC 12)

DDSN shall implement mechanisms to ensure availability of information in the event of the loss of cryptographic keys by users.

DDSN shall implement mechanisms to ensure the confidentiality of private keys.

DDSN shall develop a mechanism to randomly select a key from the entire key space, using hardware-based randomization.

DDSN shall implement appropriate controls to physically and logically safeguard the key-generating equipment from construction through receipt, installation, operation, and removal from service.

Cryptographic Protection (SC 17)

For Restricted or data protected by Federal or State laws or regulations: DDSN shall use Federal Information Processing Standards (FIPS)-140 validated (e.g., Advanced Encryption Standards (AES), Triple Data Encryption Algorithm (TDEA), Diffie-Hellman, RSA, Rivest Cipher 5 (RC5)) technology for encrypting confidential data.

DDSN shall implement all encryption mechanisms to comply with this policy and support a minimum of, but not limited to the industry standard, AES 128-bit encryption.

DDSN shall not use any proprietary encryption algorithms for any purpose, unless approved by DDSN's information security department.

Transmission Confidentiality and Integrity (SC 8 and SC 9)

Confidential or restricted information transmitted as an email message shall be encrypted based on DDSN encryption policy.

Any confidential or restricted information transmitted through a public network to and from vendors, customers, or entities doing business with DDSN shall be encrypted or be transmitted through a tunnel encrypted by approved technologies such as virtual private networks (VPN), point-to-point tunnel protocols (PPTP) like secure socket layers (SSL).

DDSN shall implement wireless encryption standards such as Wi-Fi Protected Access 2 (WPA2), and VPN encryption for remote wireless and/or internal network configurations to encrypt wireless transmissions that are used for transmitting confidential or restricted information.

DDSN shall utilize encrypted file transfer programs such as "secured File Transfer Protocol (SFTP)" (FTP over Secure Shell (SSH) and Secure Copy (SCP) to secure transfer of documents and data over the Internet. Only authorized users shall be able to initiate secure transactions.

Guidance: *NIST SP 800-53 Revision 4: SC 1 System and Communications Protection Policy and Procedures*
 NIST SP 800-53 Revision 4: SC 8 Transmission Integrity
 NIST SP 800-53 Revision 9: SC 8 Transmission Confidentiality
 NIST SP 800-53 Revision 4: SC 12 Cryptographic Key Establishment and Management
 NIST SP 800-53 Revision 4: SC17 Cryptographic Protection

PRIVACY

Policy Privacy Impact Assessment

DDSN shall conduct a Privacy Impact Assessment (PIA) on information systems that will handle Personal Identifiable Information (PII).

DDSN shall publish privacy policies on DDSN websites used by the public.

DDSN shall update PIAs when a system change creates new privacy risks (e.g., when functions applied to existing information collection change anonymous information into information in identifiable form).

PIAs shall include:

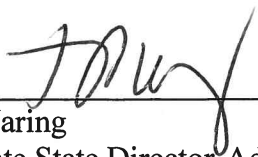
- a. What information is to be collected (e.g., nature and source);
- b. Why information is being collected (e.g., to determine eligibility)
- c. Intended use of information (e.g., to verify existing data);
- d. With whom the information will be shared;
- e. What opportunities individuals have to decline to provide information;
- f. How the information will be secured;

The PIA document shall be reviewed by a DDSN executive or designee, such as CIO, CISO, or similar.


DDSN shall provide a confidentiality agreement defining the responsibilities of the DDSN's employees and business partners (e.g., contractors, vendors) in maintaining the privacy of electronic information.

The DDSN electronic information privacy officer, in conjunction with the DDSN human resources department, is responsible for the development and administration of this confidentiality agreement.

*Guidance: Fair Information Practice Principles (FIPPs)
OMB Memorandum 03-22*



Tom Waring
Associate State Director-Administration
(Originator)



Beverly Buscemi, Ph.D.
State Director
(Approved)

***To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>***

PROPOSED TO MARK OBSOLETE

Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration



3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/LSN-INFO
Website: www.ddsn.sc.gov

COMMISSION
William O. Danielson
Chairman
Eva R. Ravenel
Vice Chairman
Gary C. Lemel
Secretary
Mary Ellen Barnwell
Sam F. Broughton, Ph.D.
Catherine O. Fayssoix
Vicki A. Thompson

Reference Number: 367-22-DD

Title of Document: Information Security Policy - Asset Management

Date of Issue: April 27, 2016
Effective Date: April 27, 2016
Last Review Date: April 27, 2016
Date of Last Revision: July 13, 2016

Applicability: All DDSN Employees (NEW)

PURPOSE

The purpose of the Asset Management Policy is to define the basis for developing an inventory of assets that support DDSN. Compiling an inventory of assets is important for judging the relative value and importance of agency assets. Based on this information, DDSN shall provide appropriate levels of protection.

I. ACCESS IDENTIFICATION

1. Information System Component Inventory (CM 8)

DDSN shall document and maintain inventories of the important assets associated with each information system. Asset inventories shall include a unique system name, a system/business owner, a data classification, and a description of the location of the asset.

Examples of assets associated with information systems are:

- **Information assets:** databases and data files, system documentation, user manuals, training material, operational procedures, disaster recovery plans, archived information;

P.O. Box 239
Clinton, SC 29325-5328
Phone: (864) 938-3497

DISTRICT I

Midlands Center - Phone: 803/935-7500
Whitten Center - Phone: 864/833-2733

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832-5576

DISTRICT II

Coastal Center - Phone: 843/873-5750
Pee Dee Center - Phone: 843/664-2600
Saleeby Center - Phone: 843/332-4104

- **Software assets:** application software, system software, development tools and utilities;
- **Physical assets:** physical equipment (e.g., processors, monitors, laptops, portable devices, tablets, smartphones), communication equipment (e.g., routers, servers), magnetic media (e.g., tapes and disks).
- **Services:** computing and communications services.

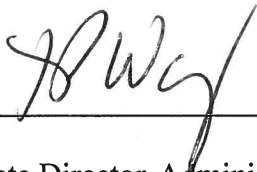
Access to DDSN assets shall be requested via a formal registration process that requires user acknowledgement of all rules and regulations pertinent to the asset.

DDSN shall periodically revalidate the asset to ensure that it is classified appropriately and that the safeguards remain valid and operative.

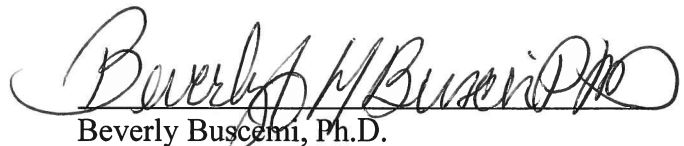
2. Security Impact Analysis (CM 4)

- DDSN shall classify assets into the data classification types in the State of South Carolina Data Classification Schema.
- DDSN shall ensure that each asset is classified based on data classification type and impact level, and the appropriate level of information security safeguards are available and in place.

Guidance: NIST SP 800-53 Revision 4: CM 4 Security Impact Analysis
NIST SP 800-53 Revision 4: CM 8 Information System Component Inventory



Tom Waring
Associate State Director-Administration
(Originator)



Beverly Buscemi, Ph.D.
State Director
(Approved)

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

PROPOSED TO MARK OBSOLETE

Beverly A. H. Buscemi, Ph.D.

State Director

David A. Goodell

Associate State Director

Operations

Susan Kreh Beck

Associate State Director

Policy

Thomas P. Waring

Associate State Director

Administration



3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240

803/898-9600

Toll Free: 888/DSN-INFO

Website: www.dds.sc.gov

COMMISSION

William O. Danielson

Chairman

Eva R. Ravenel

Vice Chairman

Gary C. Lemel

Secretary

Mary Ellen Barnwell

Sam F. Broughton, Ph.D.

Catherine O. Fayssoux

Vicki A. Thompson

Reference Number: 367-23-DD

Title of Document: Information Security Policy - Information Systems
Acquisitions, Development, and Maintenance

Date of Issue: May 3, 2016
Effective Date: May 3, 2016
Date of Last Revision: July 13, 2016

Applicability: All DDSN Employees (REVISED)

1. Change Management

The purpose of the change management is to ensure all changes are assessed, approved, implemented and reviewed in a controlled manner to production, and applicable non-production environments with minimal impact and risk.

Configuration Change Control (CM 3)

DDSN shall define change management controls to manage changes to information systems in order to minimize the likelihood of disruption, unauthorized alterations and errors. The implementation of changes shall be controlled through the use of a change control process. The following recommendations shall be followed for the change control process:

- All requests for change shall be handled in a structured way that determines the impact on the operational system and its functionality;
- All changes to production environments, including emergency maintenance and patches, shall be formally managed in a controlled manner.

DISTRICT I

P.O. Box 239
Clinton, SC 29325-5328
Phone: (864) 938-3497

Midlands Center - Phone: 803/935-7500
Whitten Center - Phone: 864/833-2733

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832-5576

DISTRICT II

Coastal Center - Phone: 843/873-5750
Pee Dee Center - Phone: 843/664-2600
Saleeby Center - Phone: 843/332-4104

- DDSN shall have a process to categorize, prioritize and authorize changes to information systems;
- Post-implementation reviews shall be performed to ensure production changes are operating as intended;
- A process shall be defined and communicated to ensure that all new modifications to the production environment have been adequately tested;
- A process for defining, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process shall be established; and
- Information systems shall be reviewed and tested after major changes to operating systems.

Guidance: NIST SP 800-53 Revision 4: CM 3 Configuration Change Control

2. Configuration Management

The purpose of the configuration management is to establish procedures for the compliance with minimally acceptable system configuration requirements, as determined by DDSN. In addition, this section helps ensure DDSN establish processes to identify and implement secure configurations, control configuration changes, and monitor security controls to validate adherence with approved configurations.

Policy Baseline Configuration (CM 2)

- DDSN shall develop, review, and formally approve baseline configurations (most secure state) for critical information systems and infrastructure components.
- DDSN shall develop a process to manage changes to baseline configurations, including identification, review, security impact analysis, test, and approval prior to implementation of changes.
- DDSN shall establish a central repository of all baseline configurations and shall implement access restrictions to prevent unauthorized changes.
- DDSN shall retain older versions of baseline configurations to be able to support rollback.
- DDSN shall review and update baseline configurations periodically, and/or as an integral part of information system component installations or upgrades.

Configuration Management Plan (CM 9)

The DDSN shall assign responsibilities for developing and managing the configuration management process to personnel that are not directly involved in system development activities.

Guidance *NIST SP 800-53 Revision 4: CM 2 Baseline Configuration*
NIST SP 800-53 Revision 4: CM 9 Configuration Management Plan
NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems

3. System Development and Maintenance

The purpose of system development and maintenance is to define requirements for system security planning and to improve protection of DDSN information system resources.

Policy System Security Plan (PL 2)

- DDSN shall prepare system security plans and documentation for critical enterprise information systems or systems under development.
- System security plans shall provide an overview of the security requirements of the system and describe the controls in place for meeting the requirements through all stages of the systems development life cycle.
- When the system is modified in a manner that affects security, system documentation shall be updated accordingly.

Vulnerability Scanning (RA 5)

- DDSN shall perform a vulnerability assessment on all enterprise information systems undergoing significant changes, before the systems are moved into production.
- DDSN shall perform periodic vulnerability assessments on production enterprise information systems and take appropriate measures to address the risks associated with any identified vulnerabilities.
- Vulnerability notifications from vendors and other appropriate sources shall be monitored and assessed for all information systems and applications.
- System and Services Acquisition Policy and Procedures (SA 2)
- DDSN shall develop and follow a set of procedures consistent with State procurement standards as defined by the Division of Information Security and the Information Technology Management Office.
- DDSN shall ensure that the State's interests have been protected and enforced in all IT procurement contracts.

System Development Life Cycle (SA 3)

- DDSN shall implement appropriate security controls at all stages of the information system life cycle.

External Information System Services (SA 9)

- DDSN shall supervise and monitor outsourced software development to validate DDSN security requirements.

Developer Security Testing and Evaluation (SA-11)

- DDSN shall establish separate development, testing, and production environments.
- DDSN shall not use production data for testing purposes unless the data has been obfuscated, sanitized, or declassified. If production data must be temporarily used in these environments, appropriate security controls, including management approval, procedures to remove/delete data after completion of tests, and documentation of activities, shall be implemented.

Flaw Remediation (SI 2)

- DDSN shall design appropriate controls into information systems, including user developed applications to ensure correct processing.
- DDSN shall ensure that software patches are applied when they function to remove or reduce security weaknesses.

Security Alerts, Advisories, and Directives (SI 5)

- DDSN shall establish a process to collect information system security alerts, advisories, and directives on patches on an ongoing basis and implement these security directives in accordance with established time frames.
- A specific group or individual shall be given responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes.

Software, Firmware, and Information Integrity (SI 7)

- DDSN shall ensure that any decision to upgrade to a new release shall take into account the business requirements for the change, and the security of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version).
- DDSN shall test critical operating system (OS) changes and updates in the test environment to ensure there is no adverse impact on organizational operations or security.

Information Input Validation (SI 10)

- DDSN shall incorporate controls into information systems to check the validity of information inputs and information outputs.
- DDSN shall incorporate processing validation checks into information systems to detect processing errors, inadvertent or deliberate processing actions (e.g., accidental deletions).

Session Authenticity (SC 23)

- DDSN shall identify the appropriate controls to ensure session authenticity, protecting message integrity in applications and protecting information transmission to and from information systems.

Policy Supplement *Threat and Vulnerability Management 1.1: Patch Management*
Threat and Vulnerability Management 1.2: Vulnerability Assessment Solution

Guidance: *NIST SP 800-53 Revision 4: PL 2 System Security Plan*
NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning
NIST SP 800-53 Revision 4: SA 2 System and Services Acquisition Policy and Procedure
NIST SP 800-53 Revision 4: SA 3 System Development Life Cycle
NIST SP 800-53 Revision 4: SA 9 External Information System Services
NIST SP 800-53 Revision 4: SA 11 Developer Security Testing and Evaluation
NIST SP 800-53 Revision 4: SI 2 Flaw Remediation
NIST SP 800-53 Revision 4: SI 7 Software, Firmware, and Information Integrity
NIST SP 800-53 Revision 4: SI 10 Information Input Validation
NIST SP 800-53 Revision 4: SC 23 Session Authenticity

4. Release Management

The purpose of release management is to define the appropriate release activities during an implementation or upgrade of information systems.

Policy Allocation of Resources (SA 2)

- DDSN shall ensure that production-ready release packages have been deployed using the release management lifecycle (i.e., plan, prepare, build and test, pilot, and deploy).
- DDSN shall determine as part of the release planning process:
 - Resources required to deploy the release;
 - Pass/fail criteria;
 - Build and test plans prior to implementation;
 - Pilot and deployment plans; and
 - Develop requirements for the release.

Information System Documentation (SA 5)

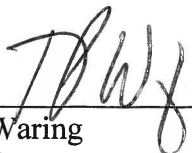
- DDSN shall document the set of tools and processes used to manage the IT release lifecycle, and the prioritization of the release;

- DDSN shall validate the release design against the requirements, and identify the risks and potential issues.

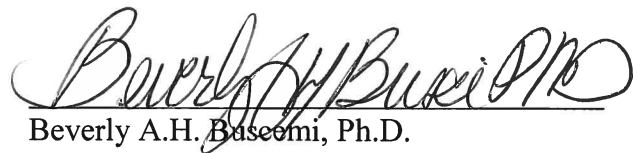
Security Engineering Principles (SA 8)

- DDSN shall implement standardization and enforce operational controls through the use of change requests for deploying releases into production.

Guidance: *NIST SP 800-53 Revision 4: SA 2 Allocation of Resources*
 NIST SP 800-53 Revision 4: SA 5 Information System Documentation
 NIST SP 800-53 Revision 4: SA 8 Security Engineering Principles



Tom Waring
Associate State Director-Administration
(Originator)



Beverly A.H. Baseem, Ph.D.
State Director
(Approved)

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

PROPOSED TO MARK OBSOLETE

Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration



3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/DSN-INFO
Website: www.ddsn.sc.gov

COMMISSION
William O. Danielson
Chairperson
Gary C. Lemel
Vice Chairman
Eva R. Ravenel
Secretary
Mary Ellen Barnwell
Sam F. Broughton, Ph.D.
Catherine O. Fayssoux
Vicki A. Thompson

Reference Number: 367-24-DD
Title of Document: Information Security Policy – IT Compliance
Date of Issue: June 1, 2016
Effective Date: June 1, 2016
Last Review Date: June 1, 2016
Date of Last Revision: June 1, 2016
Applicability: All DDSN Employees (NEW)

PURPOSE

The purpose of the IT Compliance policy is to establish controls and process to maximize the effectiveness and minimize interference to/from the information systems audit process while providing effective monitoring and response capabilities in relation to incidents. This will ensure compliance with information security policies and standards at DDSN.

I. AUDIT AND COMPLIANCE

Compliance with Legal and Contractual Requirements (A.15.1)

DDSN shall identify and document its obligations to applicable State, federal and other third party laws and regulations in relation to information security.

Compliance with Security Policies and Standards (A.15.2.1, A.15.2.2)

At least annually, DDSN shall perform reviews or audits of users' and systems' compliance with security policies, standards, and procedures, and initiate corrective actions where necessary.

Results from compliance reviews or audits shall be documented, and reported to DDSN leadership.

DISTRICT I

P.O. Box 239
Clinton, SC 29325 5328
Phone: (864) 938 3497

Midlands Center - Phone: 803/935 7500
Whitten Center - Phone: 864/833 7733

DISTRICT II

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832 5576

Coastal Center - Phone: 843/873 5750
Pee Dee Center - Phone: 843/664 2600
Saleeby Center - Phone: 843/332 4104

Audit and Accountability Policy and Procedures (AU 1)

DDSN shall establish a formal, documented audit and accountability policy and associated audit and accountability procedures.

DDSN shall implement a process to review and update the audit and accountability policy and associated procedures at least annually.

Guidance: *ISO 27001:2005: A.15.1 Compliance with legal and contractual requirements*
 ISO 27001:2005: A.15.2.1 Compliance with security policies and standards
 ISO 27001:2005: A.15.2.2 Technical compliance checking
 NIST SP 800-53 Revision 4: AU 1 Audit and Accountability Policy and Procedures

II. INFORMATION SYSTEM AUDIT CONSIDERATIONS

Information Systems Audit Controls (A.15.3.1)

DDSN shall implement audit procedures to help ensure that activities involving reviews or audits of operational systems are carefully planned to minimize the risk of disruptions to business processes.

Protection of information systems audit tools (A.15.3.2)

DDSN shall implement security controls to help prevent unauthorized access and/or access abuse of audit tools.

Audit Events (AU 2)

DDSN shall determine the type of events that are to be audited within information systems.

DDSN shall review and update the list of audited events annually.

DDSN leadership shall ensure coordination between the audit function, information security function, and business functions to facilitate the identification of auditable events.

Content of Audit Records (AU 3)

DDSN information systems shall be enabled to generate audit records containing details to help establish what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of any individuals or subjects associated with the event.

Audit Records Review and Reporting (AU 6)

DDSN shall analyze information system audit records periodically.

DDSN shall report findings of audit records reviews to information security personnel and DDSN leadership.

DDSN shall perform correlation and analysis of information generated by security assessments and monitoring.

Audit Storage Capacity (AU 4)

DDSN shall allocate sufficient audit storage capacity to help ensure compliance with audit logs retention requirements from State, federal, and other applicable third party laws and regulations.

DDSN shall implement provisions for information systems to off-load audit records at regular intervals onto a different system or media than the system being audited.

Guidance: *ISO 27001:2005: A.15.3.1 Information systems audit controls*
 ISO 27001:2005: A.15.3.2 Protection of information systems audit tools
 NIST SP 800-53 Revision 4: AU 2 Audit Events
 NIST SP 800-53 Revision 4: AU 3 Content of Audit Records
 NIST SP 800-53 Revision 4: AU 4 Audit Storage Capacity
 NIST SP 800-53 Revision 4: AU 6 Audit Review, Analysis, and Reporting

III. INFORMATION SECURITY CONTINUOUS MONITORING

Policy Continuous Monitoring (CA 2)

DDSN shall employ assessment teams to monitor the security controls on an ongoing basis.

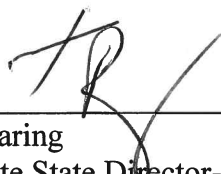
DDSN assessment teams shall be independent from operational or business functions, or hired third parties.

Plan of Action and Milestones (CA 5)

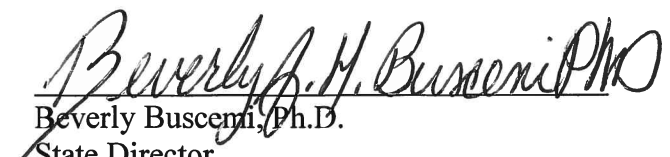
DDSN shall develop a plan of action and milestones to document planned remedial actions to correct weaknesses or deficiencies identified as result of internal/external risk assessments, security reviews, and/or audits.

DDSN shall update its plan of action and milestones at least on a yearly basis, and also based on the findings from continuous security monitoring activities.

Guidance: *NIST SP 800-53 Revision 4: CA 2 Security Assessments*
 NIST SP 800-53 Revision 4: CA 5 Plan of Action and Milestones



Tom Waring
Associate State Director-Administration
(Originator)



Beverly Busceni, Ph.D.
State Director
(Approved)

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

PROPOSED TO MARK OBSOLETE



Beverly A. H. Buscemi, Ph.D.

State Director

David A. Goodell

Associate State Director

Operations

Susan Kreh Beck

Associate State Director

Policy

Thomas P. Waring

Associate State Director

Administration

COMMISSION

William O. Danielson

Chairperson

Gary C. Lemel

Vice Chairman

Eva R. Ravenel

Secretary

Mary Ellen Barnwell

Sam F. Broughton, Ph.D.

Catherine O. Fayssoux

Vicki A. Thompson

3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600

Toll Free: 888/DSN-INFO

Website: www.ddsn.sc.gov

Reference Number: 367-25-DD

Title of Document: Information Security Policy – IT Risk Strategy

Date of Issue: June 1, 2016

Effective Date: June 1, 2016

Last Review Date: June 1, 2016

Date of Last Revision: June 1, 2016

Applicability: All DDSN Employees (NEW)

PURPOSE

The purpose of the IT Risk Strategy policy is to establish Security Controls, Performance and Metrics to evaluate the security program and Third Party Risk to DDSN information and information processing facilities that are accessed, processed, communicated to, or managed by third parties.

I. SECURITY PERFORMANCE AND METRICS

Information Security Measures of Performance (PM 6)

DDSN shall develop, monitor, and report on performance metrics to demonstrate progress in adoption of security controls, and associated policies and procedures, and effectiveness of the information security program.

DDSN-defined performance measures should be able to support the determination of information system security posture, demonstrate compliance with requirements, and identify areas of improvement.

DISTRICT I

P.O. Box 239
Clinton, SC 29325-5328
Phone: (864) 938-3497

Midlands Center - Phone: 803/935-7500
Whitten Center - Phone: 864/833-2733

DISTRICT II

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832-5576

Coastal Center - Phone: 843/873-5750
Pee Dee Center - Phone: 843/664-2600
Saleeby Center - Phone: 843/332-4104

Manageability of Metrics (3.4.2)

DDSN shall ensure that the metrics/ measures that are collected are meaningful, yield impact and outcome findings, and provide stakeholders with the time necessary to use the results to address performance gaps.

Data Management Concerns (3.4.3)

DDSN shall standardize the data collection methods and data repositories used for metrics data collection and reporting to ascertain the validity and quality of data.

*Guidance: NIST SP 800-53 Revision 4: PM 6 Information Security Measures of Performance
NIST SP 800-55 Revision 1: 3.4.2 Manageability
NIST SP 800-55 Revision 1: 3.4.3 Data Management Concerns*

II. THIRD PARTY RISK MANAGEMENT

External Information System Services (SA 9)

DDSN shall establish a policy and associated processes to enforce that third parties comply with information security requirements and employ defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

DDSN shall implement processes, methods, and techniques to monitor security control compliance by third parties on an ongoing basis.

Risk Assessment (RA 3)

DDSN shall establish a process to conduct risk assessments on third party service providers, and document the risk assessment results.

DDSN shall implement controls to help ensure that risk assessments are updated in case of major changes in scope of services or contractual changes with third parties.

System Interconnections (CA 3)

DDSN shall authorize connections from DDSN information systems to third party information systems by entering into Interconnection Security Agreements.

For each third party interface, DDSN shall document the interface characteristics, security requirements, and the nature of the information communicated.

Use of External Information Systems (AC 20)

DDSN shall establish terms and conditions for trust relationships established with other entities owning, operating, and/or maintaining external information systems.

Terms and conditions established by DDSN should control:

- Access to DDSN information systems from third party information systems; and
- Controls for processing, storing, or transmit of DDSN data using third party information systems.

DDSN shall review and update third party security agreements on an annual basis, or as defined in the contract.

Information Sharing with Third Parties (UL 2)

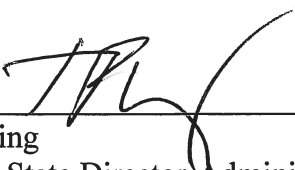
DDSN shall share personally identifiable information (PII) with third parties only for the authorized purposes identified in the Privacy Act and/or described in its notice(s), as well as State laws and Interconnection Security Agreements.

DDSN shall, where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the types of sensitive data covered (e.g., PII) and specifically enumerate the purposes for which the data may be used.


DDSN shall monitor, audit, and train its staff on the authorized sharing of sensitive data with third parties and on the consequences of unauthorized use or sharing of such data.

DDSN shall evaluate any proposed new instances of sharing sensitive data with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Guidance: *NIST SP 800-53 Revision 4: AC 20 Use of External Information Systems*
NIST SP 800-53 Revision 4: CA 3 System Interconnections
NIST SP 800-53 Revision 4: PS 6 Access Agreements
NIST SP 800-53 Revision 4: RA 3 Risk Assessment
NIST SP 800-53 Revision 4: SA 9 External Information System Services
NIST SP 800-53 Revision 4: UL 2 Information Sharing with Third Parties



Tom Waring
Associate State Director Administration
(Originator)



Beverly Busceni, Ph.D.
State Director
(Approved)

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

PROPOSED TO MARK OBSOLETE

Beverly A. H. Buscemi, Ph.D.

State Director

David A. Goodell

Associate State Director

Operations

Susan Kreh Beck

Associate State Director

Policy

Thomas P. Waring

Associate State Director

Administration



3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600

Toll Free: 888/DSN-INFO

Website: www.ddsn.sc.gov

COMMISSION

William O. Danielson

Chairperson

Gary C. Lemel

Vice Chairman

Eva R. Ravenel

Secretary

Mary Ellen Barnwell

Sam F. Broughton, Ph.D.

Catherine O. Faysoux

Vicki A. Thompson

Reference Number: 367-26-DD

Title of Document: Information Security Policy – Risk Management

Date of Issue: June 1, 2016

Effective Date: June 1, 2016

Last Review Date: June 1, 2016

Date of Last Revision: June 1, 2016

Applicability: All DDSN Employees (NEW)

PURPOSE

The purpose of the risk management policy is to define the processes and controls that shall be implemented by DDSN to identify, assess, and manage information security risks to an acceptable level. DDSN shall ensure ongoing compliance with applicable Federal and State laws and regulations.

I. RISK MANAGEMENT

Risk management typically consists of the following:

- **Risk Assessment:** A risk assessment is the first process of risk management, and is used to determine the extent of the potential threat and the risk associated with IT security.
- **Risk Mitigation:** Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls for the risks identified during the risk assessment process.

DISTRICT I

P.O. Box 239
Clinton, SC 29325-5328
Phone: (864) 938-3497

Midlands Center - Phone: 803/935-7500
Whitten Center - Phone: 864/833-2733

DISTRICT II

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832-5576

Coastal Center - Phone: 843/873-5750
Pee Dee Center - Phone: 843/664-2600
Saleeby Center - Phone: 843/332-4104

Risk Management Strategy (PM 9)

DDSN shall define a schedule for an on-going risk assessment and risk mitigation process. DDSN shall review and evaluate risk based on the system categorization level and/or data classification of their systems.

Guidance: NIST SP 800-53 Revision 4: PM 9 Risk Management Strategy

II. RISK ASSESSMENT

Policy Risk Assessment (RA 3)

The DDSN shall establish a risk assessment framework based on applicable State and federal laws, regulation, and industry standards. This assessment framework shall clearly define accountability, roles and responsibilities.

Security Assessment (CA 2)

DDSN shall annually conduct a formal assessment of the IT security processes and controls to determine the appropriateness of the design and implementation of controls, and the extent to which the controls are operating as intended and producing the desired outcome with respect to meeting the security requirements for their systems.

DDSN shall ensure that risk assessments identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the DDSN.

Plan of Action and Milestones (CA 5)

DDSN shall develop and periodically update a Plan of Action and Milestones (POAM) document that shall identify any deficiencies related to internal security controls. The POAM shall identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during annual assessments.

DDSN shall develop and periodically update a Corrective Action Plan (CAP) to identify activities planned or completed to correct deficiencies identified during the security assessment review. Both the POAM and the CAP shall address implementation of security controls to reduce or eliminate known risks in DDSN systems.

Security Authorization (CA 6)

DDSN shall establish a process and assign a senior level executive or manager to determine whether or not risks can be accepted, and for each of the risks identified following the risk assessment, the designated personnel within the DDSN shall make a decision regarding risk treatment.

Continuous Monitoring (CA 7)

DDSN shall continuously monitor the security controls within its information systems to ensure that the controls are operating as intended.

Guidance: *NIST SP 800-15*
 NIST SP 800-53 Revision 4: RA 3 Risk Assessment
 NIST SP 800-53 Revision 4: CA 2 Security Assessment
 NIST SP 800-53 Revision 4: CA 5 Plan of Action and Milestones
 NIST SP 800-53 Revision 4: CA 6 Security Authorization
 NIST SP 800-53 Revision 4: CA 7 Continuous Monitoring

III. RISK MITIGATION

Continuous Monitoring (CA 7)

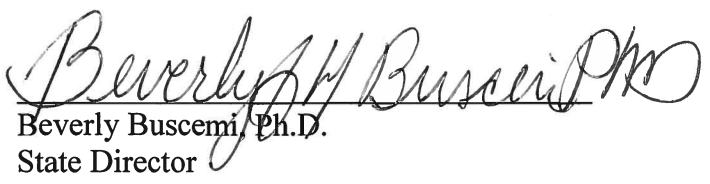
DDSN shall establish and implement controls to ensure risks are reduced to an acceptable level based on security requirements and once threats have been identified and decisions for the management of risks have been made.

DDSN shall determine and document the acceptable level for risk for various threats based on the business requirements and the impact of the potential risk to the [Agency].

Guidance: *NIST SP 800-53 Revision 4: CA 7 Continuous Monitoring*



Tom Waring
Associate State Director-Administration
(Originator)



Beverly Buscemi, Ph.D.
State Director
(Approved)

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

PROPOSED TO MARK OBSOLETE

Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration



3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/DSN-INFO
Website: www.ddsn.sc.gov

COMMISSION
William O. Danielson
Chairperson
Gary C. Lemel
Vice Chairman
Eva R. Ravenel
Secretary
Mary Ellen Barnwell
Sam F. Broughton, Ph.D.
Catherine O. Fayssoux
Vicki A. Thompson

Reference Number: 367-27-DD

Title of Document: Information Security Policy - Threat and Vulnerability Management

Date of Issue: June 1, 2016
Effective Date: June 1, 2016
Last Review Date: June 1, 2016
Date of Last Revision: June 1, 2016

Applicability: All DDSN Employees (NEW)

PURPOSE

The purpose of the Threat and Vulnerability Management policy is to establish controls and processes to help identify vulnerabilities within the DDSN technology infrastructure and information system components which could be exploited by attackers to gain unauthorized access, disrupt business operations, and steal or leak sensitive data. DDSN shall establish controls and processes that will provide information system effective monitoring capability and responsiveness against security threats and incidents. Design and implementation of an incident management framework can secure the information system against known vulnerabilities and threats. DDSN shall identify controls and processes that will provide appropriate protection against threats that could adversely affect the security of the information system or data entrusted on the information system. Effective implementation of these controls will create a consistently configured environment that is secure against known vulnerabilities in operating system and application software.

P.O. Box 239
Clinton, SC 29325 -5328
Phone: (864) 938-3497

DISTRICT I

Midlands Center -Phone: 803/935-7500
Whitten Center -Phone: 864/833-2733

DISTRICT II

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832-5576

Coastal Center -Phone: 843/873-5750
Pee Dee Center -Phone: 843/664-2600
Saleeby Center -Phone: 843/332-4104

I. VULNERABILITY ASSESSMENT

Vulnerability Scanning (RA 5)

DDSN shall implement processes to scan for vulnerabilities in information systems and hosted applications at least annually and when new vulnerabilities potentially affecting the information systems / applications are reported.

DDSN shall implement a process to control privileged access to vulnerability scanning tools and vulnerability reports.

DDSN shall analyze vulnerability scan reports and results from security control assessments.

DDSN shall remediate identified vulnerabilities in accordance with DDSN assessment of risk.

Penetration Testing (CA 8)

DDSN shall conduct penetration testing exercises on an annual basis, either by use of internal resources or employing an independent third party penetration team.

*Guidance: NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning
NIST SP 800-53 Revision 4: CA 8 Penetration Testing*

II. INCIDENT MANAGEMENT

Incident Response Policy and Procedures (IR 1)

DDSN shall develop, document, and publish an incident response policy that addresses scope, roles, and responsibilities, internal coordination efforts, and compliance.

DDSN shall establish formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

DDSN shall review and update the incident response policy and procedures on an annual basis.

Incident Response Plan (IR 8)

DDSN shall develop and/or hire a third party vendor to implement an incident response plan to:

- Establish a roadmap for implementing incident response capabilities;
- Identifies and documents the requirements of the organization, including mission, size, structure, and functions;
- Define the types of information security incidents to be reported;

- Establish metrics to help ensure incident response capabilities remain effective; and
- Define resources, such as technology and personnel, required to effectively support incident response capabilities.

DDSN shall review and update the incident response plan on an annual basis.

Incident Handling (IR 4)

DDSN shall implement formal processes to handle security incidents, including preparation, detection and analysis, containment, eradication, and recovery.

DDSN shall implement dynamic response capabilities/tools such as intrusion detection, intrusion prevention systems, and firewalls, among others, to effectively respond to security incidents.

Incident Monitoring and Reporting (IR 5, IR 6)

DDSN shall establish a process and tools to maintain detailed records of information security incidents that occur in external (e.g., boundary systems) and internal information systems.

DDSN shall implement a policy to require personnel to report suspected information security incidents to the incident response team and/or DDSN leadership.

Information System Monitoring (SI 4)

DDSN shall monitor information systems to detect attacks and/or signs of potential attacks, including unauthorized network local or remote connections.

DDSN shall deploy monitoring devices strategically within information technology environment to collect information security events and associated information.

DDSN shall protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

DDSN shall monitor inbound and outbound communications traffic to/ from the information system for unusual or unauthorized activities or conditions.

DDSN shall heighten the level of information system monitoring activity whenever there is an indication of increased risk to DDSN operations, individuals and assets,

Incident Response Training (IR 2)

DDSN shall provide incident response training within one (1) month of personnel assuming incident response roles or responsibilities.

DDSN shall provide training to incident response personnel upon significant changes to information systems and/or changes to the incident response plan.

Incident Response Testing (IR 3)

DDSN shall establish a formal process to test incident response capabilities on a yearly basis to determine the incident response effectiveness and adequacy.

DDSN shall document the incident response test results and update incident response processes as applicable.

Malicious Code Protection (SI 3)

DDSN shall employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

DDSN shall implement a process to help ensure malicious code protection mechanisms are updated whenever new releases are available.

DDSN shall configure malicious code protection mechanisms to perform periodic scans at defined time intervals.

DDSN shall block malicious code and send an alert to information system/networks administrator and initiate action(s) in response to malicious code detection.

Guidance *NIST SP 800-53 Revision 4: IR 1 Incident Response Policy and Procedures*
NIST SP 800-53 Revision 4: IR 2 Incident Response Training
NIST SP 800-53 Revision 4: IR 3 Incident Response Testing
NIST SP 800-53 Revision 4: IR 4 Incident Handling
NIST SP 800-53 Revision 4: IR 5 Incident Monitoring
NIST SP 800-53 Revision 4: IR 6 Incident Reporting
NIST SP 800-53 Revision 4: IR 8 Incident Response Plan
NIST SP 800-53 Revision 4: SI 3 Malicious Code Protection
NIST SP 800-53 Revision 4: SI 4 Information System Monitoring

III. PATCH MANAGEMENT

Flaw Remediation (SI 2)

DDSN shall develop and implement a process to identify, report, and correct information system flaws.


DDSN shall establish a formal process to test software and firmware updates related to flaw remediation for effectiveness and identification of potential impact prior to implementation.

DDSN shall install latest stable versions of applicable security software and firmware updates.

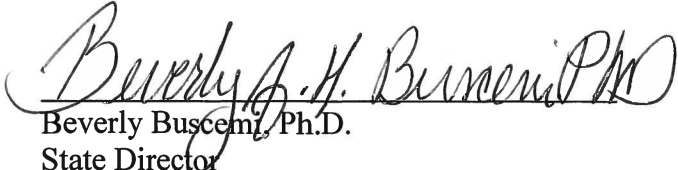
DDSN shall establish a patch cycle that guides the normal application of patches and updates to systems.

DDSN shall establish a process of patch testing to verify the source and integrity of the patch and ensure testing in a production mirrored environment for a smooth and predictable patch roll out.

Guidance: *NIST SP 800-53 Revision 4: SI 2 Flaw Remediation*
 NIST SP 800-53 Revision 4: CM 2 Baseline Configuration



Tom Waring
Associate State Director Administration
(Originator)



Beverly Buscemi, Ph.D.
State Director
(Approved)

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

PROPOSED TO MARK OBSOLETE

Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration



3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/DSN-INFO
Website: www.ddsn.sc.gov

COMMISSION
William O. Danielson
Chairperson
Gary C. Lemel
Vice Chairman
Eva R. Ravenel
Secretary
Mary Ellen Barnwell
Sam F. Broughton, Ph.D.
Catherine O. Fayssoux
Vicki A. Thompson

Reference Number: 367-28-DD
Title of Document: Information Security Policy - Business Continuity Management
Date of Issue: June 1, 2016
Effective Date: June 1, 2016
Last Review Date: June 1, 2016
Date of Last Revision: June 1, 2016
Applicability: All DDSN Employees (NEW)

PURPOSE

The purpose of the Business Continuity Management policy is to establish procedures and processes to maintain continuity of critical business operations during or post an incident or disaster. DDSN shall implement controls to identify and reduce risks, to limit the impact of damaging incidents, and to recover and restore DDSN critical business functions in a timely manner by ensuring availability of requisite resources – work location, equipment, data and technology.

I. CONTINGENCY PLANNING

Contingency Planning Policy and Procedures (CP 1)

DDSN shall establish a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

DDSN shall establish formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

DISRICT I

P.O. Box 239
Clinton, SC 29325 5328
Phone: (864) 938 3497

Midlands Center - Phone: 803/935-7500
Whitten Center - Phone: 864/833-2733

DISTRICT II

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832 5576

Coastal Center - Phone: 843/873 5750
Pee Dee Center - Phone: 843/664 2600
Saleeby Center - Phone: 843/332 4104

DDSN shall establish a formal process for annual contingency planning policy and procedure review and update.

Contingency Plan (CP 2, CP 7)

DDSN shall conduct a Business Impact Analysis (BIA) to identify functions, processes, and applications that are critical to the DDSN and determine a point in time (i.e., recovery time objective (RTO)) when the impact of an interruption or disruption becomes unacceptable to the DDSN.

DDSN shall utilize the BIA results to determine potential impacts resulting from the interruption or disruption of critical business functions, processes, and applications.

DDSN shall assign contingency roles and responsibilities to key individuals from all business functions.

DDSN shall establish procedures to maintain continuity of critical business functions despite critical information system disruption, breach, or failure.

DDSN shall document a Business Continuity Plan (BCP) that addresses documented recovery strategies designed to enable the DDSN to respond to potential disruptions and recover its critical business functions within a predetermined RTO following a disruption.

DDSN shall establish a process to ensure that the BCP is reviewed and approved by senior management.

DDSN shall distribute copies of the BCP to key personnel responsible for the recovery of the critical business functions and other relevant personnel and partners with contingency roles, as determined by the DDSN.

DDSN shall establish and implement procedures to review the BCP at planned intervals and at least on an annual basis.

DDSN shall establish a process to update the contingency plan, including BIA, when changes to the organization, information system, or environment of operation occurred.

Contingency Training (CP 3)

DDSN shall provide training to personnel with assigned contingency roles and responsibilities.

DDSN shall establish a process for identifying and delivering training requirements (i.e., frequency) to and from the relevant participants and evaluating the effectiveness of its delivery.

DDSN shall incorporate simulated events and lessons learned into contingency training to facilitate effective response by personnel with contingency roles when responding to disruption.

Contingency Plan Testing (CP 4)

DDSN shall test the BCP at least annually to determine the effectiveness of the plan and the DDSN readiness to execute the plan.

DDSN shall review the BCP test results, record lessons learned and perform corrective actions as needed.

DDSN shall employ standard testing methods, ranging from walk-through and tabletop exercises to more elaborate parallel/full interrupt simulations, to determine the effectiveness of the plan and to identify potential weaknesses in the plans.

Criticality Analysis (SA 14)

DDSN shall establish procedures to enable continuation of critical business operations while operating in emergency mode.

Guidance: *NIST SP 800-53 Revision 4: CP 1 Contingency Planning Policy and Procedures*
 NIST SP 800-53 Revision 4: CP 2 Contingency Plan
 NIST SP 800-53 Revision 4: CP 3 Contingency Training
 NIST SP 800-53 Revision 4: CP 4 Contingency Plan Testing
 NIST SP 800-53 Revision 4: SA 14 Criticality Analysis

II. DISASTER RECOVERY and CONTINGENCY STRATEGIES

Disaster Recovery Plan (CP 2)

DDSN shall develop a Disaster Recovery Plan (DRP) that addresses scope, roles, responsibilities, and coordination among organizational entities for reallocating information systems operations to an alternate location.

DDSN shall establish recovery time objectives for the BIA identified critical information systems.

DDSN shall establish and document procedures to fully restore critical information systems, post an incident, without deterioration of the security safeguards originally planned and implemented.

DDSN shall assign disaster recovery roles and responsibilities to key individuals.

DDSN shall establish a process to ensure that the DRP is reviewed and approved by senior management.

DDSN shall distribute copies of the DRP to key personnel responsible for the recovery of the critical information systems and other relevant personnel and partners with contingency roles, as determined by the DDSN.

DDSN shall establish and implement procedures to review the DRP at planned intervals and at least on an annual basis.

DDSN shall establish a process to update the DRP when changes to the organization or environment of operation occurred.

Alternate Site (CP 7)

DDSN shall identify and establish processes to relocate to an alternate site to facilitate the resumption of information system operations for business-critical functions within the defined recovery objectives (RTO and Recovery Point Objective (RPO)) when the primary site is unavailable due to disruption.

DDSN shall ensure that equipment and supplies required to resume operations at the alternate processing site are available.

DDSN shall ensure contracts are in place with third parties and suppliers to support delivery to the site within the defined time period for transfer/ resumption of critical business operations.

DDSN shall ensure that the alternate processing site provides information security safeguards similar to that of the primary site.

DDSN shall identify potential accessibility problems to the alternate site in the event of an area-wide disruption or disaster.

Telecommunications Services (CP 8)

DDSN shall establish primary and alternate telecommunication service agreements with priority-of-service provisions in accordance with organizational availability requirements (including RTOs), quality of service and access;

DDSN shall establish alternate telecommunications services to facilitate the resumption of information system operations for critical business functions within the defined recovery objectives when the primary telecommunications capabilities are unavailable.

DDSN shall require primary and alternate telecommunication service providers to have contingency plans.

Information System Recovery and Reconstitution (CP 10)

DDSN shall establish documented procedures to restore and recover critical business activities from the temporary measures adopted to support normal business requirements after an incident.

DDSN shall implement procedures for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

DDSN shall provide the capability to restore information system components within defined restoration time periods from configuration-controlled and integrity-protected information representing a known, operational state for the components (for e.g. reimaging methods).

DDSN shall establish measures to protect backup and restoration hardware, firmware, and software.

Guidance: *NIST SP 800-53 Revision 4: CP 7 Alternate Processing Site*
 NIST SP 800-53 Revision 4: CP 8 Telecommunications Services
 NIST SP 800-53 Revision 4: CP 10 Information System Recovery and Reconstitution

III. DATA BACKUPS

Data Backup and Storage Policy

DDSN shall develop, maintain and document a Data Backup and Storage Policy that address the adequate procedures to storage data and thus ensure the recovery of electronic information in the event of failure.

DDSN shall identify and apply security requirements for protecting data backups based on the different types of data (sensitive, confidential, public) handle by the entity.

Alternate Storage Site (CP 6)

DDSN shall identify an alternate storage site that is separated from the primary site so as not to be susceptible to same hazards to storage and recover information system backup information.

DDSN shall establish necessary agreements with the site/ location owner to ensure that data storage and retrieval process are not hindered during or post an incident.

DDSN shall ensure that the alternate storage site provides information security safeguards similar to that of the primary storage site.

DDSN shall identify potential accessibility problems to the alternate storage site in the event of a disruption or disaster.

DDSN shall identify secure transfer methods when transporting backup media off-site.
DDSN shall establish and maintain an authorization list to retrieve backups from the off-site location.

DDSN shall review on an annual basis the security of the off-site location to ensure data is unexposed to unauthorized disclosure or modification while in storage.

Information System Backup (CP 9)

DDSN shall establish a process to perform data backups of user-level and system-level information at a defined frequency consistent with the established RTOs and RPOs.

DDSN shall establish a process to perform data backups of information system security documentation at a defined frequency consistent with RTOs and RPOs.

DDSN shall establish safeguards and controls to protect the confidentiality, integrity, and availability of backup information at storage locations.

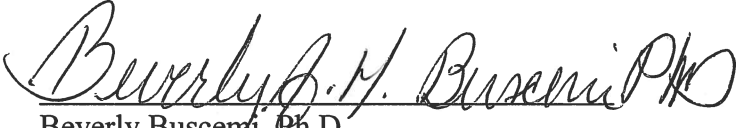
DDSN shall identify encryption/secure methods in storage of backup data to transportable media (i.e., tapes, CD Rooms, etc.).

DDSN shall enforce dual authorization (“two-person control”) for the deletion or destruction of DDSN sensitive data.

Guidance: *NIST SP 800-53 Revision 4: CP 6 Alternate Storage Site*
 NIST SP 800-53 Revision 4: CP 9 Information System Backup



Tom Waring
Associate State Director-Administration
(Originator)



Beverly Buscemi, Ph.D.
State Director
(Approved)

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

PROPOSED TO MARK OBSOLETE

Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration



3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/DSN-INFO
Website: www.ddsn.sc.gov

COMMISSION
William O. Danielson
Chairperson
Gary C. Lemel
Vice Chairman
Eva R. Ravenel
Secretary
Mary Ellen Barnwell
Sam F. Broughton, Ph.D.
Catherine O. Fayssoux
Vicki A. Thompson

Reference Number: 367-29-DD
Title of Document: Information Security Program Master Policy
Date of Issue: June 1, 2016
Effective Date: June 1, 2016
Last Review Date: June 1, 2016
Date of Last Revision: June 1, 2016
Applicability: All DDSN Employees (NEW)

PURPOSE

The purpose of this Master Policy is to establish the principles to regulate how DDSN shall provide an appropriate level of governance controls over Information Security related activities. DDSN shall establish key principles based on which DDSN's Security Organization shall be established. DDSN shall establish key principles based on which DDSN's security procedures and controls shall be developed and deployed.

I. INFORMATION SECURITY PROGRAM PLANNING

Information Security Plan (PM 1)

DDSN shall develop and communicate an information security plan that underlines security requirements, the security management controls, and common controls in place for meeting those requirements.

DDSN's security plan shall identify and assign security program roles, responsibilities and management commitment, and ensure coordination among the agency's business units, as well as compliance with the security plan.

DISTRICT I

P.O. Box 239
Clinton, SC 29325-5328
Phone: (864) 938-3497

Midlands Center - Phone: 803/935-7500
Whitten Center - Phone: 864/833-2733

9995 Miles Jamison Road
Summerville, SC 29485
Phone: 843/832-5576

DISTRICT II

Coastal Center - Phone: 843/873-5750
Pee Dee Center - Phone: 843/664-2600
Saleeby Center - Phone: 843/332-4104

DDSN shall ensure coordination among the agency's business units responsible for the different aspects of information security (i.e., technical, physical, personnel, etc.).

DDSN shall ensure that the security plan is approved by senior management.

DDSN shall review the information security plan at least on an annual basis.

DDSN shall update the security plan to address changes and problems identified during plan implementation or security control assessments.

DDSN shall protect the information security plan from unauthorized disclosure and modification

Information Security Resources (PM 3)

DDSN shall consider resources needed to implement and maintain the information security plan in capital planning and investment requests.

Plan of Action and Milestones Process (PM 4)

DDSN shall implement a process for ensuring that plans of action and milestones for the security program and associated information systems are developed and maintained.

DDSN shall review plans of action and milestones for consistency with the agency's risk management strategy and priorities for risk response actions.

Information Security Measures of Performance (PM 6)

DDSN shall develop, monitor, and report on the results of information security measures of performance, as directed or guided by the South Carolina Division of Information Security (SC DIS) and the South Carolina Enterprise Privacy Office (SC EPO).

Guidance: *NIST SP 800-53 Revision 4: PM 1 Information Security Program Plan*
 NIST SP 800-53 Revision 4: PM 3 Information Security Resources
 NIST SP 800-53 Revision 4: PM 4 Plan of Action and Milestones Process
 NIST SP 800-53 Revision 4: PM 6 Measures of Performance

II. SECURITY ORGANIZATION (ROLES and RESPONSIBILITIES)

Information Security Authority (2.2.3.1)

DDSN's chief executive shall ensure that the agency's senior officials are given the necessary authority to secure the operations and assets under their control.

Information Security Liaison (PM 2)

DDSN shall appoint an information security liaison with the mission and resources to: coordinate, develop, implement, and maintain an information security plan.

Information Security Workforce (PM 13)

DDSN shall establish an information security workforce and professional development program appropriately sized to the agency's information security needs.

Role-based Security Training (AT 3)

DDSN shall provide role-based security training to personnel with assigned security roles and responsibilities.

*Guidance: NIST SP 800-53 Revision 4: PM 2 Senior Information Security Officer
NIST SP 800-53 Revision 4: PM 13 Information Security Workforce
NIST SP 800-53 Revision 4: AT 3 Role-based Security Training
NIST SP 800-100: 2.2.3.1 Agency Head*

III. POLICY MANAGEMENT (PLAN OF ACTION)

Procedure Development

DDSN shall adopt a risk-based approach to identify State, Federal and agency-specific information security objectives, and shall develop information security procedures in alignment with the identified security objectives.

DDSN shall allocate the appropriate subject matter experts to the development of State and agency-specific information security procedures.

DDSN shall approach independent external (third party) specialists to assist in the development of information security policies in cases where it is established that the required skills do not exist within the agency and are not available within any other state government agency.

DDSN shall work in collaboration with other states, Federal government, and external special interest groups in cases where procedures directly or indirectly affect interfacing activities with them.

Information security procedures that are developed at the agency shall contain the following information, as appropriate:

- Revision history
- Introduction
- Preface
- Ownership, roles, and responsibilities

- Purpose
- Policy statements
- Policy supplement
- Guidance
- Definitions

Scenarios which cannot be effectively addressed within the constraints of the agency's security procedures, should be identified as exceptions:

- Exceptions shall be evaluated in the context of potential risk to the agency as a whole;
- Exceptions that create significant risks without adequate compensating controls shall not be approved; and
- Exceptions shall be consistently evaluated in accordance with the agency's risk acceptance practice.

DDSN shall review each draft procedure with stakeholders who shall be impacted by the procedure, to ensure that the procedure is enforceable and effective.

DDSN shall identify gaps within the procedures that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps.

DDSN shall develop and implement a communication plan to disseminate new procedures or changes to existing procedures.

DDSN shall review procedures on an annual basis to ensure that procedures are up-to-date and aligned with the State's risk posture.

Procedure Review and Approval

A procedure governance committee shall be established for the purpose of review and approval of procedures.

Procedure exemptions shall be explicitly approved by the procedure governing committee.

Procedure approval history shall be documented in detail.

Procedure Implementation

DDSN shall implement mechanisms to help ensure that information security procedures will be available to the agency's personnel on a continuous basis and whenever required.

DDSN shall require employees to review and acknowledge understanding of information security procedures prior to allowing access to sensitive data or information systems.

Guidance: NIST SP 800-53 Revision 4: PM 6 Measures of Performance

IV. INFORMATION SECURITY CONTROLS DEPLOYMENT

Controls Deployment

DDSN shall adopt a risk-based approach to prioritize deployment of controls.

DDSN shall allocate the appropriate subject matter experts to the deployment of State, Federal and agency-specific information security controls.

DDSN shall approach independent external (third party) specialists to assist in the deployment of information security controls in cases where it is established that the required skills do not exist within the agency and are not available within any other state government agency.

Controls which cannot be deployed due to the agency's resource or other constraints must be reported to the office of the State Chief Information Security Officer.

DDSN shall review each control with stakeholders who shall be impacted, to ensure that the control is enforceable and effective.

DDSN shall identify gaps within the controls that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps.

DDSN shall develop and implement a communication plan to disseminate new controls or changes to existing controls.

DDSN shall review controls on an annual basis to ensure that they are up-to-date and aligned with the State's risk posture.

DEFINITIONS

Agency, State Government: Refers to any South Carolina state agency, institution, department, division, board, commission, or authority.

Control, Information Security: Refers to any process or technology intended to reduce a security risk.

Guidance: Guidance refers to best practices and industry standards that have been used as a guide to develop the security policies and the policy supplements.

Information Security Liaison: Official responsible for carrying out the "Chief Information Officer" responsibilities within the agency under the Federal Information Security Management Act (FISMA) and serving as the primary liaison between the DIS office of the Chief Information Security Officer and the agency's authorizing officials, information system owners, and information system security officers.

Information Security Plan: The collection of procedures and other guidance developed by state government agencies to implement the SC DIS Information Security Program within the agency.

Metrics: Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.

Policy: The Information Security Policy defines appropriate controls to protect an agency's information assets from unauthorized disclosure, misuse, alteration, or destruction in a manner that ensures compliance with regulatory requirements and risk management expectations.

Policy supplement: Policy supplement assists the agencies in the actual implementation of the high level security controls defined in the policy. This defines at a granular level the baseline security controls for the agency.

Policy exemptions: Scenarios which require exemption from the existing provisions of the Security policy are called policy exemptions.

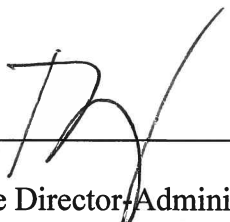
Risk posture: Risk posture identifies the specific threats that the agency faces and quantifies the risks associated with each of those threat events materializing.

SC DIS: South Carolina Division of Information Security.

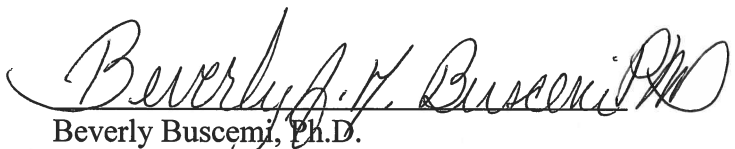
SC DIS Information Security Program: The collection of policies, procedures, and other guidance published on the SC DIS website (dis.sc.gov).

Standards: Security baseline to assist agencies, used to maintain a minimum baseline security configuration level as per industry guidelines.

System Security Plan: Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.



Tom Waring
Associate State Director, Administration
(Originator)



Beverly Buscemi, Ph.D.
State Director
(Approved)

To access any Guidance references, please see the attached link at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

Options to Address the “Gap” Issue in the Conversion of Capitated At-Home Bands B & I to Fee-for-Service

A. Background

In FY 19, DDSN’s capitated band payment system paid its 38 Boards serving as Financial Managers \$385,456,176. Of this total, \$102 million (26%) provided at-home services to 7148 individuals. On January 1, 2021, DDSN plans on converting its band payment system for “at-home” waiver services from a capitated model (Band B & Is) to a fee-for-service model (FFS).

As a result of this FFS transition on January 1, 2021, Board band payment revenues will be reduced by approximately 26% and DDSN will assume the liability from the Boards to pay FFS for the corresponding at-home services. Boards will continue to receive approximately 74% of their prospectively paid capitated band payment revenue primarily for residential services, and increased cash flow requirements from this transition are deemed manageable by most all Boards. Even though the January 1, 2021 conversion pertains to only 26% of band payment dollars, these at-home bands contain the vast majority of individual transactions needing to be converted to FFS.

B. “Gap” Issue

The conversion to FFS has many benefits as previously set forth [see Attachment A]. Our greatest conversion challenge is addressing the “Gap” issue. In FY 19 (pre-COVID-19), the Boards serving as Financial Managers (38) received \$10.4 million in Band B & I revenue in excess of Medicaid services billed. This system-wide \$10.4 million surplus “gap” was not evenly distributed to all 38 Boards [See Attachment C]. Boards had wide variability in their individual surplus (deficit) “gap” as follows:

- The average gap was a \$273,000 surplus (10% of statewide Band B & I revenues);
- Seven Boards had deficit gaps and 31 Boards had surplus gaps;
- The gap ranged from a deficit of **-\$786,549** to a surplus of \$1.19 million; and
- Individual Board’s gaps varied from -21% to 36% as a percent of their Band B & I revenue.

If DDSN stopped the Band B & I payments on January 1, 2021, without addressing this system-wide \$10.4 million surplus “gap,” the Board network revenue would be reduced by \$10.4 million. This would be de-stabilizing and have a level of unfairness. The unfairness results from DDSN’s historical failure to ever actuarially re-validate and re-balance the capitated bands. DDSN has been fully aware for the past decade that Boards generally viewed their residential bands, particularly ICFs, as underfunded, while their at-home bands generally generated annual surpluses used to supplement residential service bands.

If, on the other hand, DDSN left this \$10.4 million gap with Boards, the wide variability in Bands B & I gaps ranging from a deficit of **-\$786,549** to a surplus of \$1.19 million creates another level of unfairness. Certainly, some level of Board’s positive gaps (\$273,000 average surplus) may be needed within a Board to address their residential band funding shortfalls. However, there is also a likelihood an excessive positive gap (e.g., \$1.19 million) is unjustified and just windfall revenue of the capitated model. Given Boards are just administrators of at-home bands, the disparity of net surpluses/deficits has a level of unfairness.

C. An Unrelated but Positive Factor to Help Transition Bands B & I Conversion to FFS on January 1, 2021

As a condition of entering into an administrative cost contract with SCDHHS, DDSN must eliminate its current “split rate” administrative cost recovery model (e.g., SCDHHS’s \$31.29 Day rate to DDSN & DDSN’s lower \$27.50 Day rate to Boards) and must pass-through SCDHHS’s full service rates to Providers sometime in FY21, retroactive to July 1, 2020. This then permits DDSN to transition to a more stable administrative cost contract with SCDHHS in FY21. Passing-through the SCDHHS service rates to Boards (e.g., Day Services; ICF) will annually generate \$6.4 million new Board system revenues.

These rate increases will have to be accomplished through an increase to Provider (Boards & contracted service providers) residential band rates and increases in FFS rates for at-home services totaling \$8 million. Timing these rate increases to coincide with the at-home FFS conversion on January 1, 2021 adds substantial financial “cushion” to mitigate the FFS transition negatively impacting each Boards’ current revenue levels.

DDSN will be able to fund these new \$6.4 million annualized pass-through rate revenues to Boards from its anticipated \$8 million in new DDSN revenues from this SCDHHS FY21 administrative contract. This \$8 million will be new DDSN revenues, because DDSN’s current excess Medicaid costs in the system has negated the Medicaid matching benefit (50%) for Central Office administrative costs for many years. Additionally, DDSN is required to make retroactive payments to Boards for rate increases since July 1, 2020 through December 31, 2020, which is estimated at \$3.2 million.

D. Mandatory Board Assessments to Streamline & Prepare for Future Market Residential Rates

Under all options, DDSN will require all Boards and contracted residential service providers to undergo mandatory technical assistance. Providers will self-administer a DDSN review program to assess each of their residents’ acuity and service level, as well as agency overhead costs. DDSN will validate these self-assessments and assist providers in their respective analyses to streamline operations in preparation for FFS.

Accurate assessment of residents’ acuity levels are a key component to identify streamlining and cost savings opportunities, as well as posture each Provider to transition into future market residential rates. Each Board will recalibrate each resident’s acuity-based needs, and then internally recalibrate residents’ existing bands to the proper acuity band. This preparation of “truing up” each provider’s residential portfolio will facilitate moving to market based residential rates while also minimizing the risk of Board revenue losses.

Under all options, a safety net (e.g., loan or grant) will be provided for a minimum of six months to permit these assessments be completed and streamlining opportunities to begin implementation. By June 30, 2020, DDSN will be able to accurately gauge each Board’s need to continue their respective safety net gap grant or interest free loan, and if so, to what extent. Any safety net gap grant or interest free loan, in whole or part, to continue beyond June 30, 2021, will need to be approved by the Commission. Unjustified safety net gaps, in whole or part, will be titrated down after June 30, 2021 in a manner to minimize de-stabilizing the Board. Safety net gaps will be transitioned out of existence as residential rates are adjusted upwards in the future towards market rates, which may occur before or after the six month safety net period.

E. Options to Address the “Gap” Issue

Staff developed three options, which generally vary on how much of the \$16.8 million available revenues (\$10.4 million gap & \$6.4 million pass-through rates) are reinvested by DDSN into the Board revenue system and how the funds are allocated on January 1, 2021. These three options are as follows (see Attachment D for financial summary of options):

Gap Option #1: Pass-through the \$6.4 million SCDHHS rates (\$5.7 million Day; \$700,000 ICF) to Boards as required by SCDHHS. DDSN takes back the \$10.4 million gap (\$11.5 million surpluses - \$1.1 million deficits) and offers interest-free repayable loans to Boards with positive gaps as each streamlines operations to adjust to their new lower revenue streams.

This “rip the Band-Aid off” option does not recognize the positive gap funds as justified based on many Boards without substantial positive gap funds continued to operate at acceptable service levels. Under this option, 25 positive gap Boards will experience revenue losses. DDSN will provide access to interest-free loans to provide time for these Boards to streamline and minimize risk of destabilizing the system. The Board system has \$64 million in cash reserves, so many Boards should be able to have adequate cash available during their streamlining process [see Attachment B]. The \$64 million in cash reserves may be indicative, in part, of gap fund benefits. These loans will need to be repaid in a

methodical manner with repayment terms that are manageable consistent with the safety net described in section “D” above.

DDSN recovers the \$11.5 million positive gap funds and absorbs the \$1.1 million deficit gap funds from Boards, which nets to \$10.4 million in reserves. DDSN will need reserves inasmuch as DDSN is assuming the increase utilization risk by accepting the liability to pay all at-home services. Boards’ cost control tension on balancing individuals needed services with capitated dollars will be gone, while the FFS model will now incentivize service utilization requiring additional state funds by DDSN.

Gap Option #2: DDSN will Pass-through the \$6.4 million SCDHHS rates (\$5.7 million Day; \$700,000 ICF) to Boards as required by SCDHHS. DDSN takes back the \$10.4 million gap (\$11.5 million surpluses - \$1.1 million deficits), but then gives each Board a grant equal to each Board’s revenue reduction to re-establish their gap funds through the safety net described in section “D” above. DDSN will absorb the 7 Boards’ \$1.1 million deficit gap.

This option recognizes gap funds have a role in fairly funding Boards to potentially fund current deficits in other operations or Boards in good faith used these “extra” funds to enhance services as emphasized by DDSN’s capitated model. The required pass-through rates are not placed on top of gap funds, but rather netted against gap funds to still create adequate DDSN reserves (\$3.6 million) needed to protect itself against utilization increases. Total cost will be \$13.2 million [\$11.5 million (31 Board positive gap) + \$1.1 million (absorbing 7 Boards’ deficit gap) + \$0.6 million (7 deficit Boards & 6 positive gap Boards’ pass-through rates greater than gaps)] and DDSN will generate \$3.6 million in reserves.

Gap Option #3: DDSN will Pass-through the \$6.4 million SCDHHS rates (\$5.7 million Day; \$700,000 ICF) to Boards as required by SCDHHS. DDSN takes back the \$10.4 million gap, but then reallocates \$9.8 million in a more equitable manner to address known system weaknesses in the Day rate, ICF rate, and the bed vacancy policy. Despite the Board system revenue increasing by \$5.8 million under this option, the more equitable reallocation will still adversely impact those high positive gap Boards resulting in less revenues after the transition. Boards with reduced revenues will be given grants to re-establish gap funds through the safety net described in section “D” above.

This option essentially has DDSN eliminate the gap issue, but reallocate the gap funds in a more equitable manner to address common system needs (\$9.8 million; 94%) coupled with the pass-through rates to “raise the revenue level” by \$5.8 million (56% above \$10.4 million gap) to minimize de-stabilizing the Boards. This option generates 23 Boards with increased revenues above their gap funding level and 15 with reduced revenues. Of these 15 Boards, 9 have revenue reductions of less than \$100,000 and 6 Boards greater than \$100,000. Even by adding \$5.8 million above the \$10.4 million gap baseline, 15 Boards still had reduced revenues of \$2.2 million, primarily due to their very high positive gaps. 7 of these 15 Boards have high cash reserves to support their \$1.5 million reduced revenues, while 8 Boards had \$700,000 reduced revenues and problematic cash reserves (de-stabilization risk).

This option leaves DDSN with \$2.1 million in reserves to address safety net costs [\$16.8M - \$9.8M - \$6.4M + \$1.5M (current bed vacancy cost)], as well as the anticipated utilization increases as payment for waiver services shifts to DDSN from the Boards.

The \$9.8 million reallocation addresses the following system issues:

- Add \$1.8 million to SCDHHS’s pass-through Day rate of \$31.29 to increase the rate to \$32.50. The \$32.50 rate will be a 20% increase from Boards’ current \$27.50 rate, which creates an equitable 20% vacancy rate needed for Day services to be truly a fair FFS rate. This parallels the DDSN’s existing and long-standing paid vacancy rate of 20%.

- Add \$5.1 million to SCDHHS's ICF pass-through rate of \$295.17 to increase the rate to \$324.06. This will be an annualized increase of \$12,000 per ICF bed to address this chronically unfair rate generating financial stress in the delivery system.
- Add \$2.9 million to the residential bands through the elimination of the current 60-day bed vacancy policy. The bed vacancy policy supplement is not consistent with a FFS model and undermines expediting placements from the Critical Needs List (CNL). The COVID-19 60-day bed vacancy level adds an additional \$1.45 million cost on top of the existing \$1.45 million annual cost to support the current 30 days bed vacancy policy. This also positions DDSN well for the next phase of FFS, which is flipping the remaining residential bands to FFS in the future. DDSN plans on leaving these funds in the residential bands until residential rates are adjusted to market.

F. Staff Recommendation

Staff recommends Option #2 based on the following rationale:

Option #1 is the minimum “rip the Band-Aid off” option by having DDSN take back the \$10.4 million gap and just pass-through the mandatory \$6.4 million SCDHHS pass-through rates. Downside risks include:

- Creates system de-stabilizing risk when 25 positive gap Boards (66%) will experience revenue reductions.
- Creates partnership risk between DDSN and the Boards when the new payment system causes the majority (66%) of Boards to experience revenue reductions on “day 1.”
- Creates excessive DDSN cash reserves by pulling back \$10.4 million from Boards compared to DDSN’s immediate liability in a COVID-19 environment with depressed service utilization and FMAP reserves.
- Creates a level of unfairness because the capitated system, by design, permits providers to reallocate funds within their operations where needed. The capitated system built fiscal reliance among the different bands, so pulling out two band generating a surplus leaves many Boards with only deficit bands.

Option #3 balances raising system revenues to minimize Board revenue reductions that could be de-stabilizing the service delivery system, yet still prepares for FFS by equitably rebalancing gap funds to address system weaknesses (e.g., ICF flawed rate; Day rate without an adequate vacancy factor; and eliminates the bed vacancy policy). It also identifies and stimulates action from Boards with suspected inefficiencies in residential operations due to very high positive gaps. Despite this option having many positive attributes, downside risks include:

- Creates partnership risk between DDSN and the Boards when the new payment system causes 15 Boards (40%) to experience revenue reductions on “day 1.”
- It leaves DDSN with only \$2.5 million in reserves to address initial safety net costs \$2.2 million and the risk of increase utilization.

Option #2 maintains maximum system stability. The required pass-through rates are not placed on top of gap funds, but rather netted against gap funds to create adequate DDSN initial reserves (\$3.6 million) needed to protect itself against utilization increases. Option #3 is the next best option with many positive attributes, but it adds more risk due to complexity, 15 Boards (40%) losing revenues, and less DDSN reserves for contingencies.

Attachment A

Below are the benefits of moving from a capitated Band payment system to a fee-for-service model:

- more efficient matching of state funds with Medicaid funds to increase the overall delivery system's revenue without the need for additional state appropriations;
- unwind the ineffective and costly "split rate" model to generate revenue for DDSN administrative costs and move to a more stable administrative funding model through a direct Medicaid match contract with SCDHHS;
- increase transparency;
- increase simplicity of operating the service delivery system;
- increase equity and fairness between Board Providers and contracted service Providers;
- promote market-based incentives and competition to support Provider network efficiencies;
- eliminate DDSN financial risk during COVID-19 from not generating Medicaid match revenue from at-home capitated bands caused by reduced and less predictable at-home utilization patterns;
- reduce and ultimately eliminate financial risks from one-way cost settlements with SCDHHS;
- increase linkage of tying financial success to providing quality services to individuals;
- address non-compliance risk with federal requirements for Organized Health Care Delivery System; and
- reduce the administrative burden on Boards serving as Financial Managers.

Attachment B

Analysis fo FY19-Year End Cash Reserves				
Boards	Total Cash & Investment Reserve	Total Expenses	Number of Months of Cash & Investment Reserves	Quartile Analysis of Cash & Investment Reserves by Month
Jasper DSNB	\$ -	\$ 3,338,995	-	Lowest 25% Quartile: 0.16 Month Reserve (3% Provider Statewide Reserves)
TDC Aiken*	\$ 80,133	\$ 18,921,338	0.05	
CHESCO Services	\$ 128,255	\$ 26,266,859	0.06	
Allendale/Barnwell DSNB	\$ 57,143	\$ 8,323,574	0.08	
Chester/Lancaster DSNB	\$ 58,776	\$ 7,794,098	0.09	
Dorchester Board of DSN	\$ 186,843	\$ 13,226,198	0.17	
Williamsburg DSNB	\$ 66,982	\$ 4,080,877	0.20	
Colleton DSNB	\$ 199,896	\$ 7,083,034	0.34	
Thrive Upstate (Greenville)	\$ 1,026,908	\$ 28,353,514	0.43	
Darlington DSNB	\$ 290,330	\$ 5,844,169	0.60	2nd Lowest 25% Quartile: 1.26 Month Reserve (17% Provider Statewide Reserves)
Charles Lea Center*	\$ 1,669,899	\$ 32,302,719	0.62	
Marion-Dillon BDSN****	\$ 756,969	\$ 7,940,754	1.14	
Oconee DSNB	\$ 910,195	\$ 8,907,516	1.23	
Burton Center	\$ 2,306,209	\$ 19,912,603	1.39	
Anderson DSNB	\$ 1,339,916	\$ 11,398,414	1.41	
Hampton DSNB	\$ 276,735	\$ 2,196,552	1.51	
Laurens DSNB****	\$ 1,435,362	\$ 11,362,384	1.52	
Sumter DSNB	\$ 1,426,498	\$ 10,941,230	1.56	
Fairfield Board of DSN	\$ 758,564	\$ 5,562,586	1.64	2nd Highest 25% Quartile: 2.38 Months Reserve (31% Provider Statewide Reserves)
Florence DSNB	\$ 2,209,904	\$ 15,554,205	1.70	
Georgetown DSNB	\$ 934,674	\$ 5,827,165	1.92	
Calhoun DSNB	\$ 1,100,184	\$ 6,460,978	2.04	
Union DSNB	\$ 853,372	\$ 4,530,255	2.26	
Pickens DSNB	\$ 1,712,447	\$ 8,401,415	2.45	
Lee DSNB	\$ 1,198,043	\$ 5,871,256	2.45	
York DSNB	\$ 3,825,341	\$ 17,487,849	2.62	
DBoard of Charleston	\$ 5,874,915	\$ 26,609,407	2.65	
Kershaw DSNB	\$ 891,460	\$ 3,870,429	2.76	Highest 25% Quartile: 3.91 Months Reserve (49% Provider Statewide Reserves)
Cherokee DSNB	\$ 1,353,986	\$ 5,394,423	3.01	
Horry Board of DSN****	\$ 2,807,768	\$ 11,107,742	3.03	
Orangeburg DSNB*	\$ 3,691,268	\$ 14,235,995	3.11	
Newberry DSNB	\$ 2,058,504	\$ 6,804,068	3.63	
Babcock Center, Inc.*	\$ 11,621,830	\$ 38,284,258	3.64	
Clarendon DSNB	\$ 2,413,837	\$ 7,540,192	3.84	
Bamberg DSNB	\$ 1,116,777	\$ 3,426,549	3.91	
Aiken DSNB	\$ 434,551	\$ 1,282,670	4.07	
Berkeley Citizens, Inc.**	\$ 4,606,774	\$ 12,412,035	4.45	Highest 25% Quartile: 3.91 Months Reserve (49% Provider Statewide Reserves)
Richland-Lexington DSNB	\$ 1,857,322	\$ 4,941,784	4.51	
Marlboro DSNB	\$ 760,593	\$ 1,864,178	4.90	
Total	\$ 64,299,163	\$ 435,664,267	n/a	n/a
Averages	\$ 1,648,696	\$ 11,117,878	1.78	n/a

Attachment C

Analysis of Boards' FY2019 Gap Surplus (Deficits)					
Board Name	FY2019 Surplus (Deficit) From Bands B & I	Variability Measure #1		Variability Measure #2	
		FY2019 Total Expenses	Ratio of FY2019 Surplus (Deficit)/ FY2019 Total Expenses	FY 2019 Bands B & I Revenue	Ratio of FY2019 Surplus (Deficit)/ FY2019 Bands B & I Revenues
Florence DSN Board	\$ (786,549)	\$ 15,554,205	-5.06%	\$ 3,622,327	-21.71%
Darlington DSN Board	\$ (180,398)	\$ 5,844,169	-3.09%	\$ 1,032,598	-17.47%
Williamsburg DSN Board	\$ (79,402)	\$ 4,080,877	-1.95%	\$ 968,875	-8.20%
Georgetown DSN Board	\$ (115,477)	\$ 5,827,165	-1.98%	\$ 1,429,888	-8.08%
Colleton DSN Board	\$ (26,606)	\$ 7,083,034	-0.38%	\$ 1,111,074	-2.39%
Chester/Lancaster DSN Board	\$ (39,650)	\$ 7,794,098	-0.51%	\$ 2,411,792	-1.64%
Clarendon DSN Board	\$ (13,103)	\$ 7,540,192	-0.17%	\$ 944,010	-1.39%
Fairfield DSN Board	\$ 3,027	\$ 5,562,586	0.05%	\$ 417,112	0.73%
CHESCO Services	\$ 19,301	\$ 26,266,859	0.07%	\$ 1,344,450	1.44%
Kershaw DSN Board	\$ 54,149	\$ 3,870,429	1.40%	\$ 1,945,988	2.78%
Orangeburg DSN Board	\$ 106,492	\$ 14,235,995	0.75%	\$ 2,539,443	4.19%
Babcock Center, Inc.	\$ 718,017	\$ 38,284,258	1.88%	\$ 16,751,190	4.29%
Horry DSN Board	\$ 176,069	\$ 11,107,742	1.59%	\$ 3,531,502	4.99%
Marlboro DSN Board	\$ 34,097	\$ 1,864,178	1.83%	\$ 654,072	5.21%
Sumter DSN Board	\$ 104,819	\$ 10,941,230	0.96%	\$ 1,594,145	6.58%
Anderson DSN Board	\$ 270,330	\$ 11,398,414	2.37%	\$ 3,381,913	7.99%
Thrive Upstate	\$ 1,150,832	\$ 28,353,514	4.06%	\$ 10,621,065	10.84%
MaxAbilities of York County	\$ 552,966	\$ 17,487,849	3.16%	\$ 4,563,106	12.12%
Charles Lea Center	\$ 877,077	\$ 32,302,719	2.72%	\$ 6,863,333	12.78%
Marion/Dillon DSN Board	\$ 220,009	\$ 7,940,754	2.77%	\$ 1,633,233	13.47%
Hampton DSN Board	\$ 82,942	\$ 2,196,552	3.78%	\$ 609,518	13.61%
Lee DSN Board	\$ 61,767	\$ 5,871,256	1.05%	\$ 412,586	14.97%
Charleston DSN Board	\$ 1,031,122	\$ 26,609,407	3.88%	\$ 6,103,404	16.89%
Burton Center	\$ 551,416	\$ 19,912,603	2.77%	\$ 3,148,440	17.51%
Allendale/Barnwell DSN Board	\$ 185,240	\$ 8,323,574	2.23%	\$ 1,046,181	17.71%
Dorchester DSN Board	\$ 503,773	\$ 13,226,198	3.81%	\$ 2,812,899	17.91%
Pickens DSN Board	\$ 313,291	\$ 8,401,415	3.73%	\$ 1,699,916	18.43%
Cherokee DSN Board	\$ 243,047	\$ 5,394,423	4.51%	\$ 1,303,535	18.65%
Calhoun DSN Board	\$ 165,410	\$ 6,460,978	2.56%	\$ 874,016	18.93%
Union DSN Board	\$ 148,454	\$ 4,530,255	3.28%	\$ 759,931	19.54%
Laurens DSN Board	\$ 339,031	\$ 11,362,384	2.98%	\$ 1,664,678	20.37%
Oconee DSN Board	\$ 383,106	\$ 8,907,516	4.30%	\$ 1,723,436	22.23%
Jasper DSN Board	\$ 158,088	\$ 3,338,995	4.73%	\$ 665,812	23.74%
Tri-Development Center of Aiken	\$ 1,191,254	\$ 18,921,338	6.30%	\$ 4,884,192	24.39%
Beaufort DSN Board	\$ 621,542	\$ 9,269,704	6.71%	\$ 2,411,264	25.78%
Bamberg DSN Board	\$ 139,813	\$ 3,426,549	4.08%	\$ 534,626	26.15%
Berkeley Citizens, Inc.	\$ 880,197	\$ 12,412,035	7.09%	\$ 2,852,291	30.86%
Newberry DSN Board	\$ 348,387	\$ 6,804,068	5.12%	\$ 957,803	36.37%
Total	\$ 10,393,880	\$ 438,709,517	n/a	\$ 101,825,644	n/a
Average	\$ 273,523	\$ 11,544,987	2.37%	\$ 2,679,622	10.21%

Attachment D

Analysis of Options 1, 2 & 3 (All Numbers are ANNUALIZED to Maintain Comparability)																		
Boards	Gap Funds	Option #1 - Pass-Through Rates Only				Option #2 - Maintain Gap				Option #3 - Pass Through Rates & Re-Purpose Gap						Cash Reserve Analysis		
		Pass-Through Day Rate from \$27.50 to \$31.29	Pass-Through ICF Rate from \$291.19 to \$295.17	Option #1 Total Funding	Increase (Decrease) Revenue from Gap	Pass-Through Rate Funds (Option #1)	DDSN Grants	Option #2 Total Funding (Equals Gap)	Increase (Decrease) from Gap	Pass-Through Rate Funds (Option #1)	Increase Day Pass Through Rate from \$31.29 to \$32.50 to Establish 20% Vacancy	Increase ICF Pass-Through Rate from \$295.17 to \$324.06 to Increase Annual Revenue by \$12,000	Increase Residential Rate for 1% Bed Vacancy (Eliminate Per Incident Payment)	Total Option #3	Increase (Decrease) from Gap	Cash Reserves	Months of Cash Reserves	
Beaufort DSN Board	\$ 621,542	\$ 67,845	\$ -	\$ 67,845	\$ (553,697)	\$ 67,845	\$ 553,697	\$ 621,542	\$ -	\$ 67,845	\$ 21,660	\$ -	\$ 35,737	\$ 125,242	\$ (496,300)	\$ 4,606,774	5.44	
Berkeley Citizens, Inc.	\$ 880,197	\$ 157,726	\$ 23,243	\$ 180,969	\$ (699,228)	\$ 180,969	\$ 699,228	\$ 880,197	\$ -	\$ 180,969	\$ 50,356	\$ 168,718	\$ 86,392	\$ 486,435	\$ (393,762)	\$ 3,833,088	4.45	
Charleston DSN Board	\$ 1,031,122	\$ 355,062	\$ 11,622	\$ 366,684	\$ (664,438)	\$ 366,684	\$ 664,438	\$ 1,031,122	\$ -	\$ 366,684	\$ 113,358	\$ 84,359	\$ 159,970	\$ 724,370	\$ (306,752)	\$ 5,874,915	2.65	
Tri-Development Center of A	\$ 1,191,254	\$ 295,273	\$ 46,486	\$ 341,760	\$ (849,494)	\$ 341,760	\$ 849,494	\$ 1,191,254	\$ -	\$ 341,760	\$ 94,269	\$ 337,435	\$ 138,094	\$ 911,558	\$ (279,696)	\$ 80,133	0.05	
Pickens DSN Board	\$ 313,291	\$ 75,276	\$ -	\$ 75,276	\$ (238,015)	\$ 75,276	\$ 238,015	\$ 313,291	\$ -	\$ 75,276	\$ 24,033	\$ -	\$ 62,690	\$ 161,999	\$ (151,292)	\$ 1,712,447	2.45	
Oconee DSN Board	\$ 383,106	\$ 136,756	\$ -	\$ 136,756	\$ (246,350)	\$ 136,756	\$ 246,350	\$ 383,106	\$ -	\$ 136,756	\$ 43,661	\$ -	\$ 58,362	\$ 238,778	\$ (144,328)	\$ 910,195	1.23	
Thrive Upstate	\$ 1,150,832	\$ 227,885	\$ 69,730	\$ 297,615	\$ (853,217)	\$ 297,615	\$ 853,217	\$ 1,150,832	\$ -	\$ 297,615	\$ 72,755	\$ 506,153	\$ 182,178	\$ 1,058,701	\$ (92,131)	\$ 1,026,908	0.43	
Jasper DSN Board	\$ 158,088	\$ 57,139	\$ -	\$ 57,139	\$ (100,949)	\$ 57,139	\$ 100,949	\$ 158,088	\$ -	\$ 57,139	\$ 18,242	\$ -	\$ 21,720	\$ 97,101	\$ (60,987)	\$ (119,715)	(0.43)	
Newberry DSN Board	\$ 348,387	\$ 76,510	\$ 17,432	\$ 93,942	\$ (254,445)	\$ 93,942	\$ 254,445	\$ 348,387	\$ -	\$ 93,942	\$ 24,427	\$ 126,538	\$ 51,309	\$ 296,217	\$ (52,170)	\$ 2,058,504	3.63	
MaxAbilities of York County	\$ 552,966	\$ 293,476	\$ -	\$ 293,476	\$ (259,490)	\$ 293,476	\$ 259,490	\$ 552,966	\$ -	\$ 293,476	\$ 93,696	\$ -	\$ 116,998	\$ 504,170	\$ (48,796)	\$ 3,825,341	2.62	
Hampton DSN Board	\$ 82,942	\$ 23,102	\$ -	\$ 23,102	\$ (59,840)	\$ 23,102	\$ 59,840	\$ 82,942	\$ -	\$ 23,102	\$ 7,376	\$ -	\$ 11,142	\$ 41,620	\$ (41,322)	\$ 276,735	1.51	
Marion/Dillon DSN Board	\$ 220,009	\$ 98,196	\$ -	\$ 98,196	\$ (121,813)	\$ 98,196	\$ 121,813	\$ 220,009	\$ -	\$ 98,196	\$ 31,350	\$ -	\$ 50,976	\$ 180,522	\$ (39,487)	\$ 756,969	1.14	
Dorchester DSN Board	\$ 503,773	\$ 139,025	\$ 23,243	\$ 162,268	\$ (341,505)	\$ 162,268	\$ 341,505	\$ 503,773	\$ -	\$ 162,268	\$ 44,385	\$ 168,718	\$ 91,598	\$ 466,968	\$ (36,805)	\$ 186,843	0.17	
Charles Lea Center	\$ 877,077	\$ 386,449	\$ 17,432	\$ 403,881	\$ (473,196)	\$ 403,881	\$ 473,196	\$ 877,077	\$ -	\$ 403,881	\$ 123,378	\$ 126,538	\$ 200,695	\$ 504,170	\$ (22,585)	\$ 1,669,899	0.62	
Bamberg DSN Board	\$ 139,813	\$ 82,130	\$ -	\$ 82,130	\$ (57,683)	\$ 82,130	\$ 57,683	\$ 139,813	\$ -	\$ 82,130	\$ 26,221	\$ -	\$ 28,370	\$ 136,720	\$ (3,093)	\$ 1,116,777	3.91	
Marlboro DSN Board	\$ 34,097	\$ 25,615	\$ -	\$ 25,615	\$ (8,482)	\$ 25,615	\$ 8,482	\$ 34,097	\$ -	\$ 25,615	\$ 8,178	\$ -	\$ 9,938	\$ 43,731	\$ 9,634	\$ 760,593	4.90	
Anderson DSN Board	\$ 270,330	\$ 168,401	\$ -	\$ 168,401	\$ (101,929)	\$ 168,401	\$ 101,929	\$ 270,330	\$ -	\$ 168,401	\$ 53,764	\$ -	\$ 68,741	\$ 290,906	\$ 20,576	\$ 1,339,916	1.41	
Kershaw DSN Board	\$ 54,149	\$ 45,260	\$ -	\$ 45,260	\$ (8,889)	\$ 45,260	\$ 8,889	\$ 54,149	\$ -	\$ 45,260	\$ 14,450	\$ -	\$ 20,139	\$ 79,849	\$ 25,700	\$ 891,460	2.76	
Cherokee DSN Board	\$ 243,047	\$ 60,200	\$ 23,243	\$ 83,443	\$ (159,604)	\$ 83,443	\$ 159,604	\$ 243,047	\$ -	\$ 83,443	\$ 19,219	\$ 168,718	\$ 34,301	\$ 305,682	\$ 62,635	\$ 1,353,986	3.01	
Fairfield DSN Board	\$ 3,027	\$ 38,194	\$ -	\$ 38,194	\$ 35,167	\$ 38,194	\$ -	\$ 38,194	\$ 35,167	\$ 38,194	\$ 12,194	\$ -	\$ 42,915	\$ 93,303	\$ 90,276	\$ 758,564	1.68	
Union DSN Board	\$ 148,454	\$ 92,470	\$ 11,622	\$ 104,092	\$ (44,362)	\$ 104,092	\$ 44,362	\$ 148,454	\$ -	\$ 104,092	\$ 29,522	\$ 84,359	\$ 33,674	\$ 251,646	\$ 103,192	\$ 853,372	2.26	
Laurens DSN Board	\$ 339,031	\$ 140,045	\$ 23,243	\$ 163,288	\$ (175,743)	\$ 163,288	\$ 175,743	\$ 339,031	\$ -	\$ 163,288	\$ 44,711	\$ 168,718	\$ 89,564	\$ 466,281	\$ 127,250	\$ 1,435,362	1.52	
Clarendon DSN Board	\$ (13,103)	\$ 56,012	\$ -	\$ 56,012	\$ 69,115	\$ 56,012	\$ -	\$ 56,012	\$ 69,115	\$ 56,012	\$ 17,882	\$ -	\$ 51,559	\$ 125,454	\$ 138,557	\$ 2,413,837	3.84	
Horry DSN Board	\$ 176,069	\$ 196,788	\$ -	\$ 196,788	\$ 20,719	\$ 196,788	\$ -	\$ 196,788	\$ 20,719	\$ 196,788	\$ 62,827	\$ -	\$ 58,636	\$ 318,250	\$ 142,181	\$ 2,807,768	3.03	
Williamsburg DSN Board	\$ (79,402)	\$ 65,058	\$ -	\$ 65,058	\$ 144,460	\$ 65,058	\$ -	\$ 65,058	\$ 144,460	\$ 65,058	\$ 20,770	\$ -	\$ 23,390	\$ 109,218	\$ 188,620	\$ 66,982	0.20	
CHESCO Services	\$ 19,301	\$ 80,850	\$ -	\$ 80,850	\$ 61,549	\$ 80,850	\$ -	\$ 80,850	\$ 61,549	\$ 80,850	\$ 25,812	\$ -	\$ 171,626	\$ 278,288	\$ 258,987	\$ (396,745)	(0.18)	
Georgetown DSN Board	\$ (115,477)	\$ 94,389	\$ -	\$ 94,389	\$ 209,866	\$ 94,389	\$ -	\$ 94,389	\$ 209,866	\$ 94,389	\$ 30,135	\$ -	\$ 36,029	\$ 160,552	\$ 276,029	\$ 934,674	1.92	
Lee DSN Board	\$ 61,767	\$ 82,723	\$ 23,243	\$ 105,967	\$ 44,200	\$ 105,967	\$ -	\$ 105,967	\$ 44,200	\$ 105,967	\$ 26,410	\$ 168,718	\$ 50,698	\$ 351,793	\$ 290,026	\$ 1,198,043	2.45	
Allendale/Barnwell DSN Board	\$ 185,240	\$ 94,267	\$ 34,865	\$ 129,132	\$ (56,108)	\$ 129,132	\$ 56,108	\$ 185,240	\$ -	\$ 129,132	\$ 30,096	\$ 253,076	\$ 66,379	\$ 478,683	\$ 293,443	\$ (132,842)	(0.19)	
Calhoun DSN Board	\$ 165,410	\$ 50,788	\$ 46,486	\$ 97,275	\$ (68,135)	\$ 97,275	\$ 68,135	\$ 165,410	\$ -	\$ 97,275	\$ 16,215	\$ 337,435	\$ 55,005	\$ 505,930	\$ 340,520	\$ 1,100,184	2.04	
Burton Center	\$ 551,416	\$ 180,219	\$ 69,730	\$ 249,949	\$ (301,467)	\$ 249,949	\$ 301,467	\$ 551,416	\$ -	\$ 249,949	\$ 57,537	\$ 506,153	\$ 126,230	\$ 939,868	\$ 388,452	\$ 2,306,209	1.39	
Chester/Lancaster DSN Board	\$ (39,650)	\$ 142,664	\$ 23,243	\$ 165,908	\$ 205,558	\$ 165,908	\$ -	\$ 165,908	\$ 205,558	\$ 165,908	\$ 45,547	\$ 168,718	\$ 49,162	\$ 429,335	\$ 468,985	\$ 58,776	0.09	
Darlington DSN Board	\$ (180,398)	\$ 53,758	\$ 23,243	\$ 77,001	\$ 257,399	\$ 77,001	\$ -	\$ 77,001	\$ 257,399	\$ 77,001	\$ 17,163	\$ 168,718	\$ 42,174	\$ 305,055	\$ 485,453	\$ 290,330	0.61	
Sumter DSN Board	\$ 104,819	\$ 148,863	\$ 37,770	\$ 186,633	\$ 81,814	\$ 186,633	\$ -	\$ 186,633	\$ 81,814	\$ 186,633	\$ 47,526	\$ 274,166	\$ 92,110	\$ 600,435	\$ 495,616	\$ 1,426,498	1.56	
Colleton DSN Board	\$ (26,606)	\$ 381,804	\$ -	\$ 381,804	\$ 408,410	\$ 381,804	\$ -	\$ 381,804	\$ 408,410	\$ 381,804	\$ 121,895	\$ -	\$ 48,079	\$ 551,778	\$ 578,384	\$ 199,896	0.34	
Orangeburg DSN Board	\$ 106,492	\$ 242,840	\$ 46,486	\$ 289,327	\$ 182,835	\$ 289,327	\$ -	\$ 289,327	\$ 182,835	\$ 289,327	\$ 77,529	\$ 337,435	\$ 104,275	\$ 808,566	\$ 702,074	\$ 3,691,268	3.11	
Babcock Center, Inc.	\$ 718,017	\$ 507,793	\$ 69,730	\$ 577,522	\$ (140,495)	\$ 577,522	\$ 140,495	\$ 718,017	\$ -	\$ 577,522	\$ 162,119	\$ 506,153	\$ 255,170	\$ 1,500,964	\$ 782,947	\$ 11,621,830	3.64	
Florence DSN Board	\$ (786,549)	\$ 242,597	\$ 58,108	\$ 300,705	\$ 1,087,254	\$ 300,705	\$ -	\$ 300,705	\$ 1,087,254	\$ 300,705	\$ 77,452	\$ 421,794	\$ 115,005	\$ 914,955	\$ 1,701,504	\$ 2,209,904	1.70	
Total	\$ 10,393,880	\$ 5,663,449	\$ 700,201	\$ 6,363,650	\$ (4,030,230)	\$ 6,363,650	\$ 6,838,576	\$ 13,202,226	\$ 2,808,346	\$ 6,363,650	\$ 1,808,119	\$ 5,082,618	\$ 2,941,031	\$ 16,195,418	\$ 5,801,538	\$ 65,005,678	1.92	
Summary of Each Option's Costs																Increase (Decrease) from Gap		
OPTION #1	\$ -			\$ 6,363,650							\$ -	\$ -	\$ -			\$ (4,030,230)		
OPTION #2	\$ -					\$ 6,363,650	\$ 6,838,576	\$ 13,202,226			\$ -	\$ -	\$ -			\$ 2,808,346		
OPTION #3	\$ -									\$ 6,363,650	\$ 1,808,119	\$ 5,082,618	\$ 2,941,031	\$ 16,195,418	\$ 5,801,538			
NOTE: ALL CHART NUMBERS ARE ANNUALIZED TO MAINTAIN COMPARABILITY & FACILITATE CONSISTENT BI-MONTHLY BAND PAYMENT CALCULATIONS; ANY SIX-MONTH GUARANTEED "SAFETY NET" GRANT WILL BE 50% OF THE ANNUALIZED GRANT AMOUNT ON CHART.																		

Analysis of Options 1, 2 & 3 (All Numbers are ANNUALIZED to Maintain Comparability)

Boards	Gap Funds	Option #1 - Pass-Through Rates Only				Option #2 - Maintain Gap				Option #3 - Pass Through Rates & Re-Purpose Gap					Cash Reserve Analysis		
		Pass-Through Day Rate from \$27.50 to \$31.29	Pass-Through ICF Rate from \$291.19 to \$295.17	Option #1 Total Funding	Increase (Decrease) Revenue from Gap	Pass-Through Rate Funds (Option #1)	DDSN Grants	Option #2 Total Funding (Equals Gap)	Increase (Decrease) from Gap	Pass-Through Rate Funds (Option #1)	Increase Day Pass Through Rate from \$31.29 to \$32.50 to Establish 20% Vacancy	Increase ICF Pass-Through Rate from \$295.17 to \$324.06 to Increase Annual Revenue by \$12,000	Increase Residential Rate for 1% Bed Vacancy (Eliminate Per Incident Payment)	Total Option #3	Increase (Decrease) from Gap	Cash Reserves	Months of Cash Reserves
Beaufort DSN Board	\$ 621,542	\$ 67,845	\$ -	\$ 67,845	\$ (553,697)	\$ 67,845	\$ 553,697	\$ 621,542	\$ -	\$ 67,845	\$ 21,660	\$ -	\$ 35,737	\$ 125,242	\$ (496,300)	\$ 4,606,774	5.44
Berkeley Citizens, Inc.	\$ 880,197	\$ 157,726	\$ 23,243	\$ 180,969	\$ (699,228)	\$ 180,969	\$ 699,228	\$ 880,197	\$ -	\$ 180,969	\$ 50,356	\$ 168,718	\$ 86,392	\$ 486,435	\$ (393,762)	\$ 3,833,088	4.45
Charleston DSN Board	\$ 1,031,122	\$ 355,062	\$ 11,622	\$ 366,684	\$ (664,438)	\$ 366,684	\$ 664,438	\$ 1,031,122	\$ -	\$ 366,684	\$ 113,358	\$ 84,359	\$ 159,970	\$ 724,370	\$ (306,752)	\$ 5,874,915	2.65
Tri-Development Center of AI	\$ 1,191,254	\$ 295,273	\$ 46,486	\$ 341,760	\$ (849,494)	\$ 341,760	\$ 849,494	\$ 1,191,254	\$ -	\$ 341,760	\$ 94,269	\$ 337,435	\$ 138,094	\$ 911,558	\$ (279,696)	\$ 80,133	0.05
Pickens DSN Board	\$ 313,291	\$ 75,276	\$ -	\$ 75,276	\$ (238,015)	\$ 75,276	\$ 238,015	\$ 313,291	\$ -	\$ 75,276	\$ 24,033	\$ -	\$ 62,690	\$ 161,999	\$ (151,292)	\$ 1,712,447	2.45
Oconee DSN Board	\$ 383,106	\$ 136,756	\$ -	\$ 136,756	\$ (246,350)	\$ 136,756	\$ 246,350	\$ 383,106	\$ -	\$ 136,756	\$ 43,661	\$ -	\$ 58,362	\$ 238,778	\$ (144,328)	\$ 910,195	1.23
Thrive Upstate	\$ 1,150,832	\$ 227,885	\$ 69,730	\$ 297,615	\$ (853,217)	\$ 297,615	\$ 853,217	\$ 1,150,832	\$ -	\$ 297,615	\$ 72,755	\$ 506,153	\$ 182,178	\$ 1,058,701	\$ (92,131)	\$ 1,026,908	0.43
Jasper DSN Board	\$ 158,088	\$ 57,139	\$ -	\$ 57,139	\$ (100,949)	\$ 57,139	\$ 100,949	\$ 158,088	\$ -	\$ 57,139	\$ 18,242	\$ -	\$ 21,720	\$ 97,101	\$ (60,987)	\$ (119,715)	(0.43)
Newberry DSN Board	\$ 348,387	\$ 76,510	\$ 17,432	\$ 93,942	\$ (254,445)	\$ 93,942	\$ 254,445	\$ 348,387	\$ -	\$ 93,942	\$ 24,427	\$ 126,538	\$ 51,309	\$ 296,217	\$ (52,170)	\$ 2,058,504	3.63
MaxAbilities of York County	\$ 552,966	\$ 293,476	\$ -	\$ 293,476	\$ (259,490)	\$ 293,476	\$ 259,490	\$ 552,966	\$ -	\$ 293,476	\$ 93,696	\$ -	\$ 116,998	\$ 504,170	\$ (48,796)	\$ 3,825,341	2.62
Hampton DSN Board	\$ 82,942	\$ 23,102	\$ -	\$ 23,102	\$ (59,840)	\$ 23,102	\$ 59,840	\$ 82,942	\$ -	\$ 23,102	\$ 7,376	\$ -	\$ 11,142	\$ 41,620	\$ (41,322)	\$ 276,735	1.51
Marion/Dillon DSN Board	\$ 220,009	\$ 98,196	\$ -	\$ 98,196	\$ (121,813)	\$ 98,196	\$ 121,813	\$ 220,009	\$ -	\$ 98,196	\$ 31,350	\$ -	\$ 50,976	\$ 180,522	\$ (39,487)	\$ 756,969	1.14
Dorchester DSN Board	\$ 503,773	\$ 139,025	\$ 23,243	\$ 162,268	\$ (341,505)	\$ 162,268	\$ 341,505	\$ 503,773	\$ -	\$ 162,268	\$ 44,385	\$ 168,718	\$ 91,598	\$ 466,968	\$ (36,805)	\$ 186,843	0.17
Charles Lea Center	\$ 877,077	\$ 386,449	\$ 17,432	\$ 403,881	\$ (473,196)	\$ 403,881	\$ 473,196	\$ 877,077	\$ -	\$ 403,881	\$ 123,378	\$ 126,538	\$ 200,695	\$ 854,492	\$ (22,585)	\$ 1,669,899	0.62
Bamberg DSN Board	\$ 139,813	\$ 82,130	\$ -	\$ 82,130	\$ (57,683)	\$ 82,130	\$ 57,683	\$ 139,813	\$ -	\$ 82,130	\$ 26,221	\$ -	\$ 28,370	\$ 136,720	\$ (3,093)	\$ 1,116,777	3.91
Marlboro DSN Board	\$ 34,097	\$ 25,615	\$ -	\$ 25,615	\$ (8,482)	\$ 25,615	\$ 8,482	\$ 34,097	\$ -	\$ 25,615	\$ 8,178	\$ -	\$ 9,938	\$ 43,731	\$ 9,634	\$ 760,593	4.90
Anderson DSN Board	\$ 270,330	\$ 168,401	\$ -	\$ 168,401	\$ (101,929)	\$ 168,401	\$ 101,929	\$ 270,330	\$ -	\$ 168,401	\$ 53,764	\$ -	\$ 68,741	\$ 290,906	\$ 20,576	\$ 1,339,916	1.41
Kershaw DSN Board	\$ 54,149	\$ 45,260	\$ -	\$ 45,260	\$ (8,889)	\$ 45,260	\$ 8,889	\$ 54,149	\$ -	\$ 45,260	\$ 14,450	\$ -	\$ 20,139	\$ 79,849	\$ 25,700	\$ 891,460	2.76
Cherokee DSN Board	\$ 243,047	\$ 60,200	\$ 23,243	\$ 83,443	\$ (159,604)	\$ 83,443	\$ 159,604	\$ 243,047	\$ -	\$ 83,443	\$ 19,219	\$ 168,718	\$ 34,301	\$ 305,682	\$ 62,635	\$ 1,353,986	3.01
Fairfield DSN Board	\$ 3,027	\$ 38,194	\$ -	\$ 38,194	\$ 35,167	\$ 38,194	\$ -	\$ 38,194	\$ 35,167	\$ 38,194	\$ 12,194	\$ -	\$ 42,915	\$ 93,303	\$ 90,276	\$ 758,564	1.68
Union DSN Board	\$ 148,454	\$ 92,470	\$ 11,622	\$ 104,092	\$ (44,362)	\$ 104,092	\$ 44,362	\$ 148,454	\$ -	\$ 104,092	\$ 29,522	\$ 84,359	\$ 33,674	\$ 251,646	\$ 103,192	\$ 853,372	2.26
Laurens DSN Board	\$ 339,031	\$ 140,045	\$ 23,243	\$ 163,288	\$ (175,743)	\$ 163,288	\$ 175,743	\$ 339,031	\$ -	\$ 163,288	\$ 44,711	\$ 168,718	\$ 89,564	\$ 466,281	\$ 127,250	\$ 1,435,362	1.52
Clarendon DSN Board	\$ (13,103)	\$ 56,012	\$ -	\$ 56,012	\$ 69,115	\$ 56,012	\$ -	\$ 56,012	\$ 69,115	\$ 56,012	\$ 17,882	\$ -	\$ 51,559	\$ 125,454	\$ 138,557	\$ 2,413,837	3.84
Horry DSN Board	\$ 176,069	\$ 196,788	\$ -	\$ 196,788	\$ 20,719	\$ 196,788	\$ -	\$ 196,788	\$ 20,719	\$ 196,788	\$ 62,827	\$ -	\$ 58,636	\$ 318,250	\$ 142,181	\$ 2,807,768	3.03
Williamsburg DSN Board	\$ (79,402)	\$ 65,058	\$ -	\$ 65,058	\$ 144,660	\$ 65,058	\$ -	\$ 65,058	\$ 144,660	\$ 65,058	\$ 20,770	\$ -	\$ 23,390	\$ 109,218	\$ 188,620	\$ 66,982	0.20
CHESCO Services	\$ 19,301	\$ 80,850	\$ -	\$ 80,850	\$ 61,549	\$ 80,850	\$ -	\$ 80,850	\$ 61,549	\$ 80,850	\$ 25,812	\$ -	\$ 171,626	\$ 278,288	\$ 258,987	\$ (396,745)	(0.18)
Georgetown DSN Board	\$ (115,477)	\$ 94,389	\$ -	\$ 94,389	\$ 209,866	\$ 94,389	\$ -	\$ 94,389	\$ 209,866	\$ 94,389	\$ 30,135	\$ -	\$ 36,029	\$ 160,552	\$ 276,029	\$ 934,674	1.92
Lee DSN Board	\$ 61,767	\$ 82,723	\$ 23,243	\$ 105,967	\$ 44,200	\$ 105,967	\$ -	\$ 105,967	\$ 44,200	\$ 105,967	\$ 26,410	\$ 168,718	\$ 50,698	\$ 351,793	\$ 290,026	\$ 1,198,043	2.45
Allendale/Barnwell DSN Board	\$ 185,240	\$ 94,267	\$ 34,865	\$ 129,132	\$ (56,108)	\$ 129,132	\$ 56,108	\$ 185,240	\$ -	\$ 129,132	\$ 30,096	\$ 253,076	\$ 66,379	\$ 478,683	\$ 293,443	\$ (132,842)	(0.19)
Calhoun DSN Board	\$ 165,410	\$ 50,788	\$ 46,486	\$ 97,275	\$ (68,135)	\$ 97,275	\$ 68,135	\$ 165,410	\$ -	\$ 97,275	\$ 16,215	\$ 337,435	\$ 55,005	\$ 505,930	\$ 340,520	\$ 1,100,184	2.04
Burton Center	\$ 551,416	\$ 180,219	\$ 69,730	\$ 249,949	\$ (301,467)	\$ 249,949	\$ 301,467	\$ 551,416	\$ -	\$ 249,949	\$ 57,537	\$ 506,153	\$ 126,230	\$ 939,868	\$ 388,452	\$ 2,306,209	1.39
Chester/Lancaster DSN Board	\$ (39,650)	\$ 142,664	\$ 23,243	\$ 165,908	\$ 205,558	\$ 165,908	\$ -	\$ 165,908	\$ 205,558	\$ 165,908	\$ 45,547	\$ 168,718	\$ 49,162	\$ 429,335	\$ 468,985	\$ 58,776	0.09
Darlington DSN Board	\$ (180,398)	\$ 53,758	\$ 23,243	\$ 77,001	\$ 257,399	\$ 77,001	\$ -	\$ 77,001	\$ 257,399	\$ 77,001	\$ 17,163	\$ 168,718	\$ 42,174	\$ 305,055	\$ 485,453	\$ 290,330	0.61
Sumter DSN Board	\$ 104,819	\$ 148,863	\$ 37,770	\$ 186,633	\$ 81,814	\$ 186,633	\$ -	\$ 186,633	\$ 81,814	\$ 186,633	\$ 47,526	\$ 274,166	\$ 92,110	\$ 600,435	\$ 495,616	\$ 1,426,498	1.56
Colleton DSN Board	\$ (26,606)	\$ 381,804	\$ -	\$ 381,804	\$ 408,410	\$ 381,804	\$ -	\$ 381,804	\$ 408,410	\$ 381,804	\$ 121,895	\$ -	\$ 48,079	\$ 551,778	\$ 578,384	\$ 199,896	0.34
Orangeburg DSN Board	\$ 106,492	\$ 242,840	\$ 46,486	\$ 289,327	\$ 182,835	\$ 289,327	\$ -	\$ 289,327	\$ 182,835	\$ 289,327	\$ 77,529	\$ 337,435	\$ 104,275	\$ 808,566	\$ 702,074	\$ 3,691,268	3.11
Babcock Center, Inc.	\$ 718,017	\$ 507,793	\$ 69,730	\$ 577,522	\$ (140,495)	\$ 577,522	\$ 140,495	\$ 718,017	\$ -	\$ 577,522	\$ 162,119	\$ 506,153	\$ 255,170	\$ 1,500,964	\$ 782,947	\$ 11,621,830	3.64
Florence DSN Board	\$ (786,549)	\$ 242,597	\$ 58,108	\$ 300,705	\$ 1,087,254	\$ 300,705	\$ -	\$ 300,705	\$ 1,087,254	\$ 300,705	\$ 77,452	\$ 421,794	\$ 115,005	\$ 914,955	\$ 1,701,504	\$ 2,209,904	1.70
Total	\$ 10,393,880	\$ 5,663,449	\$ 700,201	\$ 6,363,650	\$ (4,030,230)	\$ 6,363,650	\$ 6,838,576	\$ 13,202,226	\$ 2,808,346	\$ 6,363,650	\$ 1,808,119	\$ 5,082,618	\$ 2,941,031	\$ 16,195,418	\$ 5,801,538	\$ 65,005,678	1.92

OPTION #	Summary of Each Option's Costs													Increase (Decrease) from Gap		
OPTION #1	\$ -			\$ 6,363,650							\$ -	\$ -	\$ -	\$ (4,030,230)		
OPTION #2	\$ -					\$ 6,363,650	\$ 6,838,576	\$ 13,202,226			\$ -	\$ -	\$ -	\$ 2,808,346		
OPTION #3	\$ -									\$ 6,363,650	\$ 1,808,119	\$ 5,082,618	\$ 2,941,031	\$ 16,195,418	\$ 5,801,538	

NOTE: ALL CHART NUMBERS ARE ANNUALIZED TO MAINTAIN COMPARABILITY & FACILITATE CONSISTENT BI-MONTHLY BAND PAYMENT CALCULATIONS; ANY SIX-MONTH GUARANTEED "SAFETY NET" GRANT WILL BE 50% OF THE ANNUALIZED GRANT AMOUNT ON CHART.

Emails from three Boards re feedback on DDSN's three options to address the "GAP" issue when converting Bands B&I to fee-for-service presented on 11/12/2020.

Two Boards for option #2 and one Board for option #1.

BI DISCUSSION

Michelle Shaffer <mshaffer@MaxAbilities.org>

Thu 11/12/2020 11:45 AM

To: Maley, Pat <pmaley@ddsn.sc.gov>

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Good morning Pat,

Wanted to reach out to thank you, Mary and Chris for the opportunity to review the Band B/I conversion in depth. I feel like I have received good information and options to consider that truly helped me to understand the needs of and role of our agency in this conversion. While change is always difficult and I am sure we will have a steep learning curve ahead of us in the coming months, I think that Option 2 is one that we can work with. It is straightforward and allows us to provide documentation to help ensure that we can do the work with the funds received moving forward. Thank you again for working with us to help us understand the intricacies of this topic.

Michelle



Michelle Shaffer
Executive Director
7900 Park Place Rd.
PO Box 549
York, SC 29745
803-818-6752 (office)
803-230-1738 (cell)
mshaffer@maxabilities.org

Please visit:

www.yorkcoffeeroastery.com

Coffee with a Mission – order some today!

Band B and I

Jason Tavenner <jtavenner@lcdsnb.org>

Thu 11/12/2020 2:07 PM

To: Maley, Pat <pmaley@ddsn.sc.gov>

Cc: Poole, Mary <mary.poole@ddsn.sc.gov>

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Pat,

I would like to thank you and Mary for the manner in which you included Provider input into the Band B and I conversion.

The process was very helpful to understanding the many components of the decision.

After review of the options spreadsheet made available this morning, the Laurens County DSN Board would like to express our support of Option #2 – Maintain Gap.

We support this option because it seems the most equitable to all Providers and this option raises the awareness level of the “gap” but does not add undo financial pressure during the ongoing pandemic.

I remain hopeful that DDSN and DHHS will find solutions to raise DDSN’s rates, generate more match dollars and ultimately be able to pass those dollars along in service rates to Providers.

Respectfully submitted by,

Jason Tavenner
Executive Director
Laurens County DSN Board

11/12/2020

Question on the conversion chart

Elizabeth Krauss <ekrauss@gcbdsn.com>

Thu 11/12/2020 2:50 PM

To: Maley, Pat <pmaley@ddsn.sc.gov>

Cc: 'Judy Johnson' <jjohnson4444@outlook.com>

📎 1 attachments (444 KB)

DDSN Option for Band B and I Conversion.pdf;

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi Pat:

After reviewing the spreadsheet, Georgetown(45) does not support option 2. We have been doing everything we possibly can to be open in day program and serving those who want this service. Our attendance is pretty good but Option 2 doesn't reward (incentivize) us for this effort. It holds harmless those providers who have been closed. We would see no benefit for the efforts we have made to stay open or am I misinterpreting the spreadsheet? I would only support options 3 or 1.

I understood this to be short term solution, I interpreted it to be the 6 months to 6/30/21?

I would prefer a longer term solution like opt 3, that is annualized. I am assuming State government will not give DDSN any increases given the shortfalls in the new year.

I wonder when we will get the final calculations on what is being taken from Day for the first quarter?

Elizabeth Krauss
843-904-6303

From: Judy Johnson [mailto:j.johnson4444@outlook.com]

Sent: Thursday, November 12, 2020 10:54 AM

To: Adrianna K. McCullar <Adrianna@carolinabehaviorandbeyond.com>; bbeasley@ucpsc.org; bethbunge@brightstartsc.com; bjones@ncdsnb.org; bparker@barnwellsc.com; cbright@Babcockcenter.org; cgreene@cssllc.org; cpinckney@columbusorg.com; Craig A. Byrd <craig.byrd@chsgroupsc.com>; dana.mcconnell@cdservices.org; djohnson@fcdsn.org; dredd@colletondsn.org; dwalsh@jcbdsn.com; dwilush@ucpga.org; ekrauss@gcbdsn.com; Elaine Mathis <asn-sc@att.net>; ethena@pcbdsn.org; eturner@dsncc.com; fdozier@wcdsnb.org; gkeith@mddsn.org; Grady Evans <gevans@uniondsn.org>; hfrye@bciservices.org; hwaddell@Aikentdc.org; Jameson Dormann <Jdormann@sunrisegroup.org>; Jason Tavenner <jtavenner@lcdsnb.org>; jbernard@charleslea.org; jerrellynnking@acdsnb.org; Jerry Mize <jmize@thetribblecenter.com>; John Hitchman <jhitchman@scdsnb.org>; jtavenner@lcdsnb.org; Kathleen M. Childs <kchilds@sunrisegroup.org>; Kevin.wright@thementornetwork.com; Kimberly Tumbleson <kimberlytumbleson2014@yahoo.com>; kwillis@mcdsn.com; Laconda Moore <Laconda.Moore@comop.org>; Laura Collins <lcollins@fairfielddsn.net>; Lcordell@burtoncenter.org; Lindsey Daniel <Lindsey.Daniel@comop.org>; Madavis@maxhealth.com; margie@arcsc.org; Melinda@arcmidlands.org; Melissa_D_Myers23@hcbdsn.org; Michelle Shaffer <mshaffer@maxabilities.org>; Nikkie Bramlett <nbramlett@cldsn.org>; pmoss@calhoundsnb.org; Rblocker@dcdsnb.org; rcourtney@aikentdc.org; rway@ccdsnb.org; Samantha Kriegshauser <samanthak@aecenters.org>; sejohnson@rldsn.org; Shwood@Maxhealth.com; sjett@lcdsn.org; sloan@pathfindersteamsservices.com; Susan John (sujohn@hcdsn.org) <sujohn@hcdsn.org>; suzanne@beyondearlyintervention.com; t.rogers@chescoservices.org; tdavis@bcdsnb.org; teritodd@brightstartsc.com; Trex@thriveupstate.org; twarren@babcockcenter.org; Vonda Steward <Vsteward@ocdsnb.org>; wlove@bcgov.net; Zenobia Corley 2 <zcorley2759@hotmail.com>

Subject: FW: DDSN Option for Band B and I Conversion.pdf

Please read Jason's email below. Due to a time crunch, feedback is requested by Friday if possible.

Task #	Task Name	Bucket Name	Progress	Priority	Assigned To	Due Date	Description	Checklist Items
1	Establish cutoff rules related to board billed Waiver costs	Internal Fiscal Considerations	Completed	Medium	Wilson, Debra	11/20/2020	What happens when a provider pays a bill in January for a service ordered, delivered, authorized, etc before December 31?	
2	Consider how we want to handle Fiscal Agent Respite payroll for December	Internal Fiscal Considerations	Completed	Important	Wilson, Debra	11/27/2020	Need to consider payroll periods will not cleanly cut-off at 12/31. How will we settle this with providers?	
3	Provider Level Analysis - Look at 2020 numbers	Analysis	Completed	Urgent	Clark, Chris;Orner, Ben	11/13/2020	Need Ben's help to run figures by provider for 2020	
4	Establish Provider Meeting Series for Input	General To do	Completed	Important	Clark, Chris	10/02/2020	Setup Series of Meetings with Providers to Gather Ideas and Input	
5	Update waiver credit report to report only residential consumers	IT	Completed	Important	Lloyd, Donna;Bradley, Maxine	11/12/2020	To split out between at home and residential. We will only recoup those that are not at home consumers In IT requirement that need to be reviewed by business team. Already been addressed and being handled by IY. They are going to have redy for the October invoice in November	
6	Create new invoices	IT	Completed	Important	Lloyd, Donna;Bradley, Maxine;Wilson, Debra	02/06/2021	Day Programs to pay for day attendance and supported employment services In IT requirement that need to be reviewed by business team. IT has created the invoice and showed it to the team. Invoice looks good and seems to meet the criteria necessary for processing.	
7	Edit Medicare Part D report/pull back to remove B&I individuals	IT	Completed	Important	Lloyd, Donna;Orner, Ben	11/12/2020	split between residential and at home - this needs to be done as a process that needs to be created for future use when bands are flipped. In IT requirement that need to be reviewed by business team.	

Task #	Task Name	Bucket Name	Progress	Priority	Assigned To	Due Date	Description	Checklist Items
8	How will we juice the rates for other service lines to stabilize network	Analysis	Completed	Important	Clark, Chris	11/13/2020		Develop alternatives that are available to us for rate structures; Consider addressing ICF bed fees and care and maintenance reductions; Look at Residential bed vacancy funding; Consider ECTH 1 vs. CTH 1
9	Create repository for CM to send invoices	Internal Fiscal Considerations	Completed	Medium	Manos, Lori; Lloyd, Donna; Orner, Ben; Wilson, Debra	10/30/2020	Already been addressed and being handled by IT. Cannot change it yet, will confuse submitters	
10	Answer question of whether we will pay pass-through rates?	Pass Through Rates	Completed	Important	Manos, Lori; Beck, Susan K.; Orner, Ben; Ritter, Melissa; Wilson, Debra	11/06/2020	Three waivers - three rates Rate being paid higher than rate of reimbursement CS-87.8 ID 65.93 HASCI 20.30 PAY 70.59 (Hourly Employment)	
11	HOLD - Give slot/begin enrollment	Overenrollments	Completed	Medium	Manos, Lori; Orner, Ben	12/11/2020	Removing - marking as complete due to not giving them slots	
12	Need Medicare part D split by provider for FY 2019 and FY 20 Jul to Feb by Provider	IT	Completed	Important	Lloyd, Donna; Clark, Chris; Orner, Ben; Bradley, Maxine	11/13/2020		Split between Band B and I (at home) consumers vs all others (residential)
13	Add CM agency/CM to PreAuth	Env Mod Invoices	Completed	Medium	Lloyd, Donna; Orner, Ben	10/23/2020	Case Management Agency is on the form required to be submitted to us to pay, therefore why do we need it on the pre-auth. Not sure the purpose here.	
14	Rerun list of Overenrollments	Overenrollments	Completed	Medium	Bradley, Maxine; Wilson, Debra	11/27/2020	Need to coordinate timing with Carol	
15	Add CSW to Blanket open Purchase Order	Env Mod Invoices	Completed	Medium	Wilson, Debra; Mitchell, Carol	11/06/2020	current POs are for HASCI and/or IDRDR This is already done per Kelley and Nancy. Fund reservations are set up. To pay a CSW is nothing more than adding a line - nothing to worry about here.	
16	W-9 for Providers - Process	Env Mod Invoices	Completed	Medium	Orner, Ben; Wilson, Debra; Mitchell, Carol	11/06/2020	State vendor number. Can't wait until the CM sends in the invoice before we get the W-9 (at time provider added to Therap?)	
17	Analysis - provider level impact - FY 2019	Analysis	Completed	Important	Clark, Chris; Orner, Ben	09/18/2020		
18	Add DDSN as financial manager in Therap for Authorizations	Env Mod Invoices	Completed	Medium	Lloyd, Donna; Orner, Ben	09/25/2020	Therap can add this at any time.	

Task #	Task Name	Bucket Name	Progress	Priority	Assigned To	Due Date	Description	Checklist Items
19	Analyze Medicare part B/D Premium for liability purposes	Medicare B/D	Completed	Medium	Lloyd, Donna;Orner, Ben		Believe this is complete	
20	Waiver Amendment for Employment Services Group (HASCI) App K	Pass Through Rates	Completed	Medium	Manos, Lori;Beck, Susan K.;Clark, Chris;Ritter, Melissa			
21	Explore HASCI as part of new invoices	IT	Completed	Medium	Lloyd, Donna;Ritter, Melissa		Complete	
22	Analysis - statewide impact of flip	Analysis	Completed	Important	Clark, Chris;Orner, Ben			
23	Guidance for CM's	Env Mod Invoices	Completed	Medium	Manos, Lori;Orner, Ben;Ritter, Melissa			
24	Date of implementation?	Env Mod Invoices	Completed	Medium	Orner, Ben		July 1 or Oct 1?	
25	Assess impact of unusual invoice services	General To do	Completed	Medium	Manos, Lori;Orner, Ben	06/12/2020	What is the impact? In the current plans there are 65 needs that are board billed AT. 43 of those are one-time or yearly.	
26	Parking Lot - Respite to Direct bill instead?	General To do	Completed	Medium			Do we want to require boards to go to direct billed respite for the simplification of payment?	
27	Identify Overenrollments	Overenrollments	Completed	Medium	Wilson, Debra			
28	Determine if we will still fund overenrollments	Overenrollments	Completed	Medium	Clark, Chris		Chris reports we will grandfather overenrollments that currently exist in system	
29	Establish Method/Process for processing invoices for Modification/AT	Env Mod Invoices	Completed	Medium				
30	Modifications billed direct to DDSN?	Env Mod Invoices	Completed	Medium				
31	Consider impact on Cost Reports, Audit Reports, and AUP Requirements	General To do	In progress	Medium	Yacobi, Kevin;Clark, Chris	11/06/2020		
32	Are there any changes to standards or directives needed?	General To do	In progress	Important	Manos, Lori;Beck, Susan K.;Orner, Ben;Ritter, Melissa	11/06/2020		
33	Consider ability to pay providers more frequently than once per month	Internal Fiscal Considerations	In progress	Medium	Orner, Ben;Wilson, Debra	11/13/2020		Can we get billing documents out of our systems more frequently than once per month? ;Should we do a prepayment for a period of time, then reverse it later in the year?
34	Consider how we want to handle Fiscal Agent in-home support for December	Internal Fiscal Considerations	In progress	Important	Wilson, Debra	11/20/2020	Payroll period will not cutoff cleanly on December 31. How do we want to handle with Providers?	

Task #	Task Name	Bucket Name	Progress	Priority	Assigned To	Due Date	Description	Checklist Items
35	Establish procedures for providers to bill DDSN for Board Billed services	Internal Fiscal Considerations	In progress	Medium	Wilson, Debra	11/20/2020		Will they need to sign off on DSAL and logs to be paid? Can we find a better way to get approvals?;Will providers use HASCI type process to bill DDSN for respite and similar services they will be pay
36	Establish process for third party day program providers to bill DDSN Direct	Internal Fiscal Considerations	In progress	Medium	Wilson, Debra	11/20/2020	We have to be able to pay our non-DDSN board providers of day services and employment services	Communicate that private providers cannot bill for absences;Develop memo to issue to providers - Boards and Private Providers to inform them of change in bill ;Provider third party day program contracts need to be cancelled
37	Establish Process for Providers to Bill DDSN Direct	Internal Fiscal Considerations	In progress	Medium	Clark, Chris;Wilson, Debra	11/13/2020		Consider what vendors will bill DDSN direct in addition to for Mod services;Communicate need to get W-9 so vendors can be setup;Establish process to share with vendors/providers
38	Consider changes needed to outlier funding directive	Internal Fiscal Considerations	In progress	Medium	Clark, Chris	11/13/2020		Directive outlining funding for at home consumers needs to be revised
39	Revise Finance Manual and Forms	Internal Fiscal Considerations	In progress	Medium	Manos, Lori;Wilson, Debra;Mitchell, Carol	11/27/2020		
40	Consider safety net/loan program to assist with transition	Analysis	In progress	Medium	Maley, Pat;Clark, Chris	11/20/2020		If a loan program, then what will agreement/arrangement look like?;Are there any approvals we need from the State level to loan funds?
41	Position for Adjusted Payment Schedules for 12/16/20 Payment	Internal Fiscal Considerations	In progress	Urgent	Clark, Chris;Wilson, Debra;Leopard, Debra	12/11/2020		Split IDRD Waiver Credit reports into Residential and At-Home and adjust recoupment;Split Medicare Part D into Residential and At- Home and adjust recoupment;Eliminate recoupment of respite ;Adjust contract amounts for revised rates;Eliminate recoupment of in-home supports;Eliminate recoupment of CS Waiver direct billed credit reports
42	Need to Address HHS Residential Rates	Pass Through Rates	In progress	Low	Maley, Pat;Clark, Chris	03/31/2021	Residential rates need to be established based on acuity level	

Task #	Task Name	Bucket Name	Progress	Priority	Assigned To	Due Date	Description	Checklist Items
43	Get with DHHS, get same rate for all waivers	Pass Through Rates	In progress	Low	Manos, Lori;Maley, Pat;Clark, Chris	03/31/2021		summarize the different services and rates for each waiver ;Rates of concern are - Employment services individual for CS and IDRD; HASCI rates
44	Determine how to fund over-enrolled individuals	Overenrollments	In progress	Medium	Manos, Lori;Clark, Chris;Orner, Ben	12/18/2020	Should probably only be funded day program based on attendance only One's getting it now will get state funds to continue at same level (day services only) determine if they have medicaid and can be put in SFCS/CSW	Need to find way to track them.
45	Adjust Contract Language	Internal Fiscal Considerations	In progress	Important	Clark, Chris;Leopard, Debra	11/06/2020		Share comments from Ralph and Susan;Remove at home adult day program 80% attendance requirement;Share word document with Janet Priest;Get provider comments and input on their suggested changes
46	Analyze affect on R2D2 reports	Internal Fiscal Considerations	In progress	Important	Lloyd, Donna;Clark, Chris;Wilson, Debra	10/30/2020	Ask Providers what reports they are using so we can identify those that we need to ensure will still function	
47	Create process/communicate day program providers to bill DDSN directly (except for residential)	Training	In progress	Medium	Clark, Chris;Wilson, Debra;Mitchell, Carol	11/13/2020		
48	Need to Difficulty of Care Rate - ADP	Pass Through Rates	In progress	Low	Manos, Lori;Beck, Susan K.;Clark, Chris;Ritter, Melissa;Britt, Rufus	03/31/2021	Appendix K? Provider Group for day program cost data.	
49	Adjust contracts based on December 31, 2020 numbers	General To do	Not started	Medium	Leopard, Debra	02/01/2021	Can't start this until after download on Dec 31	
50	Compute phase out of Band B Outliers	Outliers	Not started	Medium	Clark, Chris;Wilson, Debra	03/31/2021		Consider impact of timing of funding and underlying costs to providers;Cost settlement process needed to true up band B outliers through Dec 2020
51	Round table with Providers for training topics	Training	Not started	Medium	Clark, Chris;Wilson, Debra	11/13/2020	Survey providers?	

Task #	Task Name	Bucket Name	Progress	Priority	Assigned To	Due Date	Description	Checklist Items
52	Consider timing of Mods for Band I take back	Internal Fiscal Considerations	Not started	Medium	Clark, Chris;Wilson, Debra	03/31/2021	Concern related to Mods incurred first part of year but not fully funded at time of flip - example - mod of \$12,000 incurred by provider, we take funds from them or they have paid bill direct, then we take back 75% of the band. This will leave them upside down on these bands if we do not consider this issue	
53	Establish Method/Process for verifying billed is authorized/approved by DDSN	Internal Fiscal Considerations	Not started	Medium	Manos, Lori;Orner, Ben;Wilson, Debra	02/26/2021	automate the reporting of authorization in existence to support amount being billed	
54	Inform CMs of need to send Board Billed services to DDSN?	Training	Not started	Medium	Manos, Lori;Orner, Ben;Wilson, Debra	11/20/2020		
55	How does CS Waiver cap figure into enhanced rate?	Outliers	Not started	Medium	Manos, Lori;Beck, Susan K.;Orner, Ben;Wilson, Debra	03/31/2021	need to communicate with HHS on CSW cap being exceeded due to DOC rate and similar rate issues; also, need to develop internal processes to monitor the cap	
56	Determine assessment of high needs for DOC rate?	Pass Through Rates	Not started	Important	Manos, Lori;Beck, Susan K.;Clark, Chris;Orner, Ben;Britt, Rufus	03/31/2021		
57	Create a procedure for providers to request DOC rate for Day Programs	Outliers	Not started	Important	Manos, Lori;Clark, Chris;Ritter, Melissa;Wilson, Debra	05/31/2021	we need to develop process to identify and approve DOC rate	
58	Notify Providers of expected change in day attendance requirements	Percentage of Attendance	Not started	Medium	Clark, Chris	12/18/2020		
59	Conduct study on Day Attendance percentages and establish new expectation	Percentage of Attendance	Not started	Medium	Clark, Chris	11/20/2020	Establish day attendance requirements for other bands attending the day program	Run reports to see what residential attendance historically runs;Establish agreed upon residential attendance requirements in contracts;Discuss possible percentage requirements with Pat and Mary

SCDDSN Incident Management Report 5-year trend data for Community Residential, Day Service, and Regional Centers Thru 9/30/2020

Community Residential	FY16	FY17	FY18	FY19	FY20	5 YEAR Average	FY21 Annualized (YTD)	ANE Allegations with Comparison to Arrest Data and Administrative Findings- Community Residential FY21Q1
# of Individual ANE Allegations	459	549	579	554	587	546	404 (101)	
# of ANE Incident Reports (One report may involve multiple allegations)	370	399	404	359	387	384	296 (74)	
Rate per 100	10.0	11.7	12.5	12.5	13.0	11.9	9.0	
# ANE Allegations resulting in Criminal Arrest	7	5	20	6	11	9.8	12 (3)	
# ANE Allegations with Administrative Findings from DSS or State Long-Term Care Ombudsman	125	157	202	114	116	142.8	108 (27)	
Day Services **	FY16	FY17	FY18	FY19	FY20	5 YEAR Average	FY21 Annualized (YTD)	ANE Allegations with Comparison to Arrest Data and Administrative Findings- Day Services FY21Q1
# of Individual ANE Allegations	58	77	57	66	47	60	8 (2)	
# of ANE Incident Reports (One report may involve multiple allegations)	49	56	46	56	38	49	4 (1)	
Rate per 100	0.72	0.94	0.71	.89	.62	0.78	.03	
# ANE Allegations resulting in Criminal Arrest	0	1	3	2	1	1.4	0	
# ANE Allegations with Administrative Findings from DSS or State Long-Term Care Ombudsman	6	5	4	3	0	3.6	0	
Regional Centers	FY16	FY17	FY18	FY19	FY20	5 YEAR Average	FY21 Annualized (YTD)	ANE Allegations with Comparison to Arrest Data and Administrative Findings- Regional Centers FY21Q1
# of Individual ANE Allegations	110	146	135	139	187	143	132 (33)	
# of ANE Incident Reports (One report may involve multiple allegations)	87	104	97	102	136	105	100 (25)	
Rate per 100	15.4	17.1	19.2	20.9	28.9	20.3	20.4	
# ANE Allegations resulting in Criminal Arrest	2	2	2	2	4	2.4	4 (1)	
# ANE Allegations with Administrative Findings from DSS or State Long-Term Care Ombudsman	19	27	34	34	18	26.4	24 (8)	

**Most Day Service locations were closed during FY20Q4 and FY21Q1 due to COVID-19.

All State Agencies are Operating Under a Continuing Resolution Appropriations

FY 20/21 Legislative Authorized & Spending Plan Budget VS Actual Expenditures (as of 10/31/2020)

Funded Program - Bud	Continuing Resolution Appropriations	Adjustments	Adjusted Budget	YTD Actual Expense	Remaining Budget	Percent Expended - Target %
						33.33%
ADMINISTRATION	\$ 8,386,999	\$ 9,000	\$ 8,395,999	\$ 2,609,002	\$ 5,786,997	31.07%
PREVENTION PROGRAM	\$ 157,098	\$ -	\$ 157,098	\$ 12,500	\$ 144,598	7.96%
GREENWOOD GENETIC CENTER	\$ 15,185,571	\$ -	\$ 15,185,571	\$ 5,958,600	\$ 9,226,971	39.24%
CHILDREN'S SERVICES	\$ 12,291,594	\$ (24,000)	\$ 12,267,594	\$ 3,115,241	\$ 9,152,353	25.39%
IN-HOME FAMILY SUPP	\$ 86,302,031	\$ (6,994,000)	\$ 79,308,031	\$ 15,842,813	\$ 63,465,218	19.98%
ADULT DEV&SUPP EMPLO	\$ 83,358,338	\$ -	\$ 83,358,338	\$ 30,745,854	\$ 52,612,484	36.88%
SERVICE COORDINATION	\$ 15,166,140	\$ -	\$ 15,166,140	\$ 3,734,208	\$ 11,431,932	24.62%
AUTISM SUPP PRG	\$ 26,368,826	\$ -	\$ 26,368,826	\$ 6,308,246	\$ 20,060,580	23.92%
HD&SPINL CRD INJ COM	\$ 5,040,532	\$ -	\$ 5,040,532	\$ 1,686,600	\$ 3,353,932	33.46%
REG CTR RESIDENT PGM	\$ 77,137,897	\$ 778,417	\$ 77,916,314	\$ 26,795,919	\$ 51,120,394	34.39%
HD&SPIN CRD INJ FAM	\$ 18,965,193	\$ 2,000,000	\$ 20,965,193	\$ 6,535,612	\$ 14,429,581	31.17%
AUTISM COMM RES PRO	\$ 29,749,084	\$ 5,000,000	\$ 34,749,084	\$ 12,958,511	\$ 21,790,573	37.29%
INTELL DISA COMM RES	\$ 340,593,466	\$ (61,266)	\$ 340,532,201	\$ 115,028,758	\$ 225,503,442	33.78%
STATEWIDE CF APPRO	\$ -	\$ 49,799	\$ 49,799		\$ 49,799	0.00%
STATE EMPLOYER CONTR	\$ 29,862,643	\$ 126,653	\$ 29,989,296	\$ 11,315,817	\$ 18,673,479	37.73%
Earmarked Authorization over DDSN Spending Plan	\$ 56,235,857	\$ -	\$ 56,235,857		\$ 56,235,857	
Legislative Authorized Total	\$ 804,801,269	\$ 884,603	\$ 805,685,872	\$ 242,647,682	\$ 563,038,189	30.12%
Legislative authorization capacity above actual spending plan budget			\$ (56,235,857)		\$ (56,235,857)	
DDSN spending plan budget			\$ 749,450,015	\$ 242,647,682	\$ 506,802,333	32.38%
Percent of total spending plan budget			100.00%	32.38%	67.62%	REASONABLE
% of FY completed (expenditures) & % of FY remaining (available funds)			100.00%	33.33%	66.67%	
Difference % - over (under) budgeted expenditures			0.00%	-0.96%	0.96%	

Carry Forward + Cash Flow Analysis Indicates Sufficient Cash to Meet FY 20 Estimated Expenditure Commitments: YES ; At-Risk ; NO

Expenditures categorized to provide insight into direct service consumers costs vs. non-direct service costs:

Expenditure	FY 20 - % of total	FY 19 - % of total
Central Office Admin & Program	2.24%	2.35%
Indirect Delivery System Costs	1.03%	1.22%
Board & QPL Capital	0.04%	0.07%
Greenwood Autism Research	0.03%	0.03%
Direct Service to Consumers	96.67%	96.33%
Total	100.00%	100.00%

NOTE: Prior FY data will be calculated and presented to provide assurance as to the consistent pattern of direct service & non-direct service expenditures and explanation for increases/decreases



South Carolina Department of Disabilities and Special Needs

RECRUITMENT AND RETENTION OF NURSING PERSONNEL BONUS PROGRAM

The South Carolina Department of Disabilities & Special Needs (DDSN) operates five Intermediate Care Facilities for Individuals with Intellectual Disabilities (ICFs-IID). These facilities provide care to more than 600 individuals with specialized healthcare needs requiring 24/7 care and supervision. The demand for essential healthcare workers, specifically direct support professionals (DSPs) and nursing personnel, is a national phenomenon and this workforce crisis is exacerbated by the COVID-19 pandemic. In an effort to stabilize our workforce and maintain optimal care to our state's most vulnerable citizens, DDSN is proposing to implement recruitment and retention bonuses to mitigate crisis staffing shortages among nursing personnel. Effective November 17, 2020, the South Carolina Department of Disabilities and Special Needs (SCDDSN) requests to implement a Recruitment ("Sign-On") and Retention Bonus program with the following provisions:

Bonus Guidelines:

- Eligible applicant shall not have been employed by DDSN within the past 90 days.
- The program continuation is contingent upon agency funding availability.
- The bonus program shall not exceed \$200,000, with an efficacy review post expenditures totaling \$100,000 and receiving Commission approval to expend additional funds.
- The program's administration and continuation is at the discretion of the Commission.

Program Guidelines

- SCDDSN shall provide up to \$3,000 in bonus pay to newly hired nursing personnel. The assignment of bonus pay will occur over a 12 month period of successful employment. These recruits may include employees moving from other State agencies by transfer, promotion, or demotion. The program applies to applicants seeking full time equivalent employees (FTE) positions in the state classifications listed below.

<u>State Classification Code and Title</u>	<u>Recruitment ("Sign-On") Bonus</u>	<u>Retention Bonus</u>
EA10 Licensed Practical Nurse I	\$1,000	\$2,000
EA15 Licensed Practical Nurse II	\$1,000	\$2,000
EA20 Registered Nurse I	\$1,000	\$2,000
EA30 Registered Nurse II	\$1,000	\$2,000



Retention Bonus Payment

Subject to the terms and conditions of the Recruitment & Retention Bonus Program for Nursing personnel, DDSN will provide retention bonus payments at the completion of each of the following periods of the first year of continuous employment with DDSN.

EA10 & 15 Licensed Practical Nursing I & II

- a) The recruitment bonus in the gross amount of \$1,000 will be paid, in the Comptroller General payroll period, after the successful completion of continuous Full Time Employment (FTE) of one (1) month with DDSN.
- b) One half of the retention bonus in the gross amount of \$1,000 will be paid, in the Comptroller General payroll period, after the successful continuous FTE employment of six (6) months with DDSN.
- c) The balance of the Retention Bonus in the gross amount of \$1,000 will be paid, in the Comptroller General payroll period, after the successful continuous FTE employment of twelve (12) months with DDSN.
- d) Employee must remain in a paid status to be eligible within the 12 month period.

EA20 & EA30 Registered Nurse I & II

- a) The recruitment bonus in the gross amount of \$1,000 will be paid, in the Comptroller General payroll period, after the successful completion of continuous Full Time Employment (FTE) of one (1) month with DDSN.
- b) One half of the retention bonus in the gross amount of \$1,000 will be paid, in the Comptroller General payroll period, after the successful continuous FTE employment of six (6) months with DDSN.
- c) The balance of the Retention Bonus in the gross amount of \$1,000 will be paid, in the Comptroller General payroll period, after the successful continuous FTE employment of twelve (12) months with DDSN.
- d) Employee must remain in a paid status to remain eligible within the 12 month period.

Employees must remain actively employed and in compliance with DDSN's policies and directives pertaining to job performance and conduct as of each payout period in order to earn and receive Retention Bonus payments. The Retention Bonus payments made under this Agreement are subject to regular tax withholdings and other authorized deductions.



Forfeiture Due To Termination or Voluntary Withdrawal of Employment:

- a) *Termination by DDSN due to Reduction in Force:* In the event DDSN terminates employment due to Division of State Human Resources approved Reduction – In –Force during this Agreement period, employees shall be entitled to receive a Retention Bonus. This amount shall be payable in the Comptroller General’s payroll period subsequent to the separation date.
- b) *Termination by DDSN for Cause or Employee Resignation:* In the event that you resign your employment or are separated from DDSN employment during the Agreement Period, you will not be entitled to receive any portion of your Retention Bonus payment. For the purposes of this Agreement, the employee shall be deemed to have resigned, and DDSN shall be deemed to have terminated the employee’s employment for “cause,” if:
 - i. The employee submits a notification or letter of resignation of employment prior to the end of the Agreement Period.
 - ii. The employee is determined to have abandoned his/her position during the Agreement Period.
 - iii. The employee violates policy or procedure that leads to separation of employment in accordance with DDSN Directive 413-01-DD “Standards of Disciplinary Action” before the end date of the Agreement Period.
 - iv. The employee’s quality of work is determined to be unacceptable, in accordance with DDSN Directive, 402-01-DD “Employee Performance Management Systems (EPMS),” leading to separation from employment before the end date of the Agreement Period.
- c) The above list is not meant to be an exhaustive list of all possible scenarios; rather it provides an example of common causes of resignation and employee separation actions.

Bonus Legislation
Updated June 27, 2019

Authority	General Parameters	Type of Reward (Monetary Limits)	Are Agencies Required to Have a Policy or Plan?	Dept. of Administration Involvement
8-1-170 Group productivity incentive programs	Recognizes and rewards team accomplishments through group performance.	Monetary reward; 25% of identified savings resulting from reduced operational costs; up to a maximum of \$2,000 per employee in a fiscal year; shared equally among team members.	A policy or procedure is required to determine unit expenses or data for the year of participation.	Proposals, actual dollar savings, and names of employees receiving rewards must be reported to Department of Administration.
8-1-180 Tokens of recognition and other rewards; limit on amount per individual	Allows recognition to reward innovations or improvements by individuals or teams that enhance the quality of work or productivity or as part of employee development programs.	Non-monetary reward; public funds may be used for plaques, certificates, and other events, including meals and similar types of recognition; limited to \$50.00 for each individual.	No policy required.	No action required.
8-1-190 Pilot programs to create innovation in state government	Allows pilot programs with individual agencies or groups of agencies to create innovations in State Government.	Monetary or non-monetary reward possible; neither specified.	No policy is required (unless Department of Administration's approval includes a requirement for a policy); Department of Administration is authorized to enter into pilot programs with agencies, such as incentive pay or other innovative reward and recognition programs.	Department of Administration approves and monitors the findings and results of the pilot programs to determine if legislative recommendations should be provided to General Assembly.

Bonus Legislation
Updated June 27, 2019

Authority	General Parameters	Type of Reward (Monetary Limits)	Are Agencies Required to Have a Policy or Plan?	Dept. of Administration Involvement
8-11-190 Use of public funds to reward state employee	Allows agencies to reward innovations or improvements by individual employees or employee teams that enhance the quality of work or productivity or as a part of employee development programs of the agency.	Non-monetary reward; plaques, certificates, meals and similar types of recognition; no limit on dollar amount of non-monetary award, but must be read in conjunction with § 8-1-180 which limits the award to \$50.00 for each individual.	No policy required.	No action required.
59-101-610 Use of Funds for Lump Sum Bonus Plans	Allows public institutions of higher learning to spend revenue at levels outlined in a plan.	Lump sum bonuses with federal and other nonstate appropriated sources of revenue.	Plan required and approved by the governing body of the respective public institution of higher learning; must maintain documentation to show use of federal funds in compliance with federal law.	No action required.
Allowance for Residences & Compensation Restrictions Proviso	Allows reward programs for designated employees.	Monetary reward; public funds and/or other funds; no limits.	Written criteria approved by the agencies' governing board or commission.	Names of employees receiving an reward and the amount received must be reported annually to Department of Administration.

Bonus Legislation
Updated June 27, 2019

Authority	General Parameters	Type of Reward (Monetary Limits)	Are Agencies Required to Have a Policy or Plan?	Dept. of Administration Involvement
Employee Bonuses Proviso	Allows agencies to recognize the accomplishments and contributions of individual employees, such as contributions to increased organizational productivity, development/implementation of improved work processes, exceptional customer service, realized cost savings.	Monetary reward; lump sum bonus not to exceed \$3,000 per employee per fiscal year.	Plan required based on objective guidelines established by the Department of Administration; Agency Director has final approval for bonus.	Annual reporting to the Department of Administration is required.
Healthcare Employee Recruitment and Retention Proviso	Allows DOC, DDSN, DHEC, DHHS, DJJ, DMH and DVR to aid in recruiting and retaining healthcare workers in critical needs healthcare jobs.	Monetary reward up to \$5,000 not to exceed an accumulation of more than \$10,000 in bonuses per year.	Based on objective guidelines established by the Department of Administration.	Annual reporting to the Department of Administration is required.

Commission Briefing: Head and Spinal Cord Injury (HASCI) Waiver Waiting List

Statement of Issue: The HASCI Waiver does not currently have a waiting list. However, all funded slots have been awarded. Absent additional dedicated funding, HASCI Waiver will need to start a waiting list immediately.

Background: HASCI Waiver has 1055 funded Waiver slots of which 1037 have been enrolled leaving 18 available waiver funded slots. DDSN has awarded 58 slots pending enrollment, which includes the 18 available funded slots and 40 over-allocated slots. These 40 over-allocated slots were needed to accommodate converting (1) the transition of HASCI Rehabilitation Supports to a waiver-funded Day Program service and (2) the stagnation of waiver enrollments (process currently being re-engineered). On average over the past twelve months, 61% of individuals allocated a HASCI Waiver slot result in enrollment. As a result, it is estimated that 35 of the 58 individuals currently pending enrollment will actually enroll. This will raise enrollment to 1072 or 17 **over** the DDSN funded level of 1055 slots.

As a result, absent new funding, DDSN needs to do the following:

1. Stop awarding new HASCI waiver slots for possible enrollment immediately and create a waiting list;
2. Let the current 58 pending slots resolve to its current estimated 1072 enrollment level;
3. Let the estimated excess 17 over-enrolled slots attrit to the 1055 funded level; and
4. After reaching the 1055 funded enrollment level, start awarding one new waiver slot to a person on the waiting list for every one waiver dis-enrollment to maintain the 1055 funding level.

Option to Fund HASCI Waiver Slots Through Fiscal Year 20201 (FY21): DDSN will receive no new legislative funding in FY21. However, the General Assembly's guidance for agencies is to exercise flexibility in reallocating existing resources to meet mission needs during the COVID-19 pandemic, so consideration was given to converting existing Community Supports (CS) funded waiver slots to HASCI funded slots for the remainder of FY21. Currently, DDSN has 526 CS and 170 Intellectual Disability/Related Disabilities (ID/RD) funded waiver slots available, which totals 696. It is estimated all 170 ID/RD and 61 CS funded waiver slots will be awarded over the remaining 8 months of FY21. Absent new funding for FY22, the remaining 462 legislatively funded CS slots would meet FY22 needs and become exhausted early in FY23 (Fall 2022).

To avoid starting an immediate waiting list and fund new HASCI Waiver slots for the remaining 8 months of FY21, 27 new funded waiver slots are needed (27 new slots + 18 available slots = 45 slots needed for 8 months). If HASCI Waiver reels in its current excess slot awards and lowers pending times, a waiting list can be delayed until late in FY21. Given the average annual cost of HASCI Waiver services is \$36,500 and the CS Waiver is \$8,946 (1:4 ratio), it would take 108 CS Waiver slots to fund HASCI Waiver needs through FY21. The impact would be CS funded waiver slots would be exhausted 4 months sooner, which would be at the end of FY22.

Points for Consideration in Starting a HASCI Waiver Waiting List or Approval of the Option to Fund HASCI Waiver Slots Funding Through FY21:

- For the past six years, there has been no waiting list for the HASCI Waiver, while there has been a continual waiting list for the CS Waiver (currently at 3.2 years).
- While people with Brain and Spinal Cord Injuries often require more immediate services relative to activities of daily living, those with Intellectual and Related Disabilities and their families also need services.

- There are stakeholder considerations including the possibility of appearing to prioritize HASCI Waiver over CS Waiver participants.
- General Assembly staff have been supportive of using CS funding, but formal approval from the Executive Budget Office and relevant General Assembly leadership will be required.

Staff Recommendations: Staff recommends to start a HASCI Waiver waiting list.

STATE DIRECTOR'S REPORT

November 19, 2020

1. SFAA (State Fiscal Accountability Authority) – meets on December 17th. We have the Whitten Center property conveyance to the city of Clinton on the agenda only. The Whitten project has been in the works since – at least - 2016 and it needs to get completed. Once this one is done, we will place the transfer of the 60 programmatic properties on the agenda. We did meet with Comptroller General Eckstrom and we were able to clear up a couple of misconceptions. We will reach out again to discuss the 60 properties in more depth. As of today, we have been unable to get a meeting with a board member and/or his staff.
2. We have a Legislative Oversight Committee update due on December 13th. There was one item that was only partially done – increasing the number of DSPs. Of course, we have ramped up recruiting efforts – use of on-line recruiters such as Indeed, increasing orientations to 2x a month and increased the number of job hiring events held. We have also taken on the issue in a more long term approach - we have taken the task on as an educational issue and developed a DSP credentialing curriculum for seniors in high school. We did have 26 participants at our 2 pilot schools- of course, COVID threw a wrench in the mix and the on-site internships did not materialize. It should be known that the program has been well received by the students, school districts and DDSN providers. DDSN worked with the SC Department of Education- Office of Career and Technical Education to have the South Carolina Direct Support Professional recognized as an Industry Credential per approval from the SC Education Oversight Committee. This will allow schools and students to receive recognition for their efforts. So the heavy lifting has been done – we just need school to be operating in a manner which will let these student participate in an on-site internship that will prepare them for a career in our industry.
3. We have implemented increased information security reforms at Central Office and Regional Centers through implementing two factor authentications. This is like receiving a code from your bank via email to be used to access your bank account information. This second authentication mechanism dramatically improves are information security posture and come into compliance with state requirements. We will be rolling this out to the provider network within the next couple of months.

4. Kudos to Midlands Center and Coastal Center who both experienced an increase in COVID-19 cases. We currently have 3 residents statewide in the 14 day CDC window; 11 days ago we had 26—no fatalities. As with the entire state – the entire country, covid is staging a resurgence. There are additional cases in the community provider homes/staff also.
5. As a result of the inspections, citations and IJ at Whitten in July, DHEC has proposed issuing a fine. We are currently appealing that decision.
 - a. They came in on old complaints as well as new ones – from terminated employees
 - b. They came in and found nothing with regards to the PPE and infection control complaints save on house
 - c. Even the incident regarding the IJ – which was reported to them, prior to them coming to the facility by us, that they only investigated when there was a complaint. If this was a true IJ – why did they not come into the facility when we reported it?
 - d. The circumstances surrounding everything that happened at Whitten were covid based – so it was unprecedented to have that many staff call out. Why did they choose an unprecedented event to levy a fine –which, in itself, is unprecedented?
 - e. And the IJ was resolved as was any lingering conditions -
 - f. They did so only because of the media being involved. The fact that the media are involved in anything should never be the reason a state agency acts – and acts outside of what they normally would have done.
6. The Risk Management group – formally known as Quality management has done a lot of pre-work to get us to a point where decisions now need to be made before going further. I would ask that the Commission set a work group date in January to receive a thorough briefing on the Quality Management paradigm shift that we are proposing and the choices we have as an agency as to where we want to go from here.
7. EVV – electronic visit verification – this is a mandate set forth in the CURES act – as a means to cut down on fraud and waste in at home health care programs. The deadline to be compliant with this law is January 1, 2021. Since we are not the Medicaid agency, we have not had the opportunity to choose the system or build out the system. DHHS has chosen a system called Care Call

which is tied to their Phoenix system of case management. We were initially informed that our waiver service providers (Personal Care in folks' homes) would be included in any system chosen by HHS. We were under the impression that a new system was being sought – it just has not materialized yet. So the Care call system will be utilized. We have hit a bit of a roadblock; since we use Therap as our CM system, our authorizations are not in Phoenix and the providers for our individuals in the waiver bill HHS through a web tool and self-directed services for in home supports are billed through the fiscal agents. We are working on an acceptable solution to this issue and CMS is being engaged by HHS. Of course, as with everything DDSN, we have a unique situation here since some providers do not bill directly and even those who do bill Medicaid directly, do not bill through the Care Call system. There is a fine for non-compliance of .5 FMAP for that particular service. In home supports, PCA I and II, respite and Attendant Care. The service has to have an element of personal care involved.