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

SOUTH CAROLINA Department OF Disabilities AND Special Needs

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.

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