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:	367-24-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.

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 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