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

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.

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 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