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

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.

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