State of Iowa Enterprise Interconnectivity Security Standard

June 22, 2011

Purpose

This document provides the minimum requirements to establish, maintain, and terminate interconnections with the shared state IT infrastructure or to IT systems outside state government.

Overview

The State of Iowa maintains a variety of data in its IT systems, including confidential and sensitive customer information. Connecting agency IT systems to networks outside of their agency increases the risk of unauthorized access to information and disruption of service. Protection of data and systems will be enhanced by ensuring that agencies follow standards when connecting to the shared state IT infrastructure or to IT systems outside state government.

Scope

For the purpose of this standard, security is defined as the ability to protect the confidentiality, integrity, and availability of information processed, stored and transmitted by agencies. Information technology assets covered by this policy include those that process, store, transmit or monitor digital information. This document presents minimum standards which must be met by agencies wishing to connect to the shared State IT infrastructure and IT systems outside state government.

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions

Selected terms used in the Enterprise Interconnectivity Standard are defined below:

- **Anti-virus Software**: A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents

- **Compromise**: Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

- **Interconnection or interconnectivity:** The direct connection of two or more IT systems for the purpose of sharing data and other information resources. This includes connections to: other agencies; trading partners; third party service providers; and the Internet.

- **Penetration Test**: Security test in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network.

- **Security Controls**: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

- **Security Incident**: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies

- **Vulnerability Assessment:** Formal description and evaluation of the vulnerabilities in an information system.

Updates

This standard will be reviewed at least every two years and updated as needed.

ELEMENTS OF THE STANDARD

The following elements apply to agencies connecting to the shared State IT infrastructure or IT systems outside state government.

1. Logging: Agencies shall maintain and review logs for all servers and network devices. Agencies shall:

a. Develop a log review policy including:
   i. Length of time for log retention (Log retention must be at least 90 days)
   ii. Individual(s) responsible for log review
   iii. Log review frequency
   iv. Log review procedures
b. Develop baseline behavior for normal activity
c. Derivation of Time: Devices will synchronize their time with a NTP server. Daylight savings time will be adjusted.

2. Encryption: Agencies must use a minimum of 256 bit encryption for: remote connections; administration tasks; and file transfers containing confidential data.

3. Firewalls: Agencies shall install and maintain firewalls at all interconnections to their agency. This includes connections to: other agencies; trading partners; third party service providers; and the Internet. The following requirements must be met for firewalls:

a. Default passwords are changed before installation
b. Software and/or integrated operating systems of hardware firewalls are up to date. Updates must be tested before going into production.
c. SNMP community strings are changed from default setting
d. Firewalls shall perform ingress and egress filtering
e. Firewalls shall block all traffic by default. An exception list shall be established to identify authorized ports, services and addresses. Ports with no activity for over a year shall be closed.
f. Critical systems are segregated into logical zones

g. Firewalls must fail in a closed state
h. Firewall configurations are reviewed, and updated quarterly by network administrators

4. Logical Access Controls: Agencies shall use Access Control Lists (ACL) and access rules to specify the access for authorized personnel (or agencies if they are using a site-to-site VPN) to networked devices (servers, routers, switches and firewalls). ACLs shall include the level of access and the types of transactions and functions that are permitted (e.g., read, write, execute, delete, create, and search).

a. ACL's shall be:
    i. Configured offline
    ii. Versioned in a repository
    iii. Distributed to the appropriate control device
b. Agencies shall grant appropriate access privileges:
    i. Based on roles or job functions
    ii. Based on the principle of least privilege
c. Only system administrators with a business need have access to the controls

5. Banner: Log-on screens used for entry into an agency's network shall have a warning banner. The agency's legal counsel shall approve the banner and notify users that:
a. Users are entering a State of Iowa system
b. Access is limited to authorized use only
c. Users consent to monitoring

6. Identification and Authentication: Agencies shall identify and authenticate users to ensure that they are authorized to access the interconnection:
a. At a minimum passwords and user IDs will be used. Passwords shall be:
    i. At least eight characters and administrator passwords shall be at least 10 characters
    ii. A mixture of numbers, upper and lower case letters
    iii. Include at least one special character
    iv. Changed at least every sixty days
b. Master password files shall be encrypted and protected from unauthorized access.
c. Emergency administrator passwords shall be stored securely.
d. The following may be used in addition to strong passwords.
    i. Digital certificates
    ii. Authentication tokens
    iii. Biometrics
    iv. Smart cards

7. Virus Scanning: Agencies shall install anti-virus software on all servers and computers, except for mainframe computers. The following requirements must be met:
a. Data transferred to the agency from an external source is scanned
b. Anti-virus software automatically checks for updates at least daily
c. Administrators are notified via email, text message or pager if the anti-virus software cannot automatically clean a detected virus
d. Users are instructed on how to report a suspected virus

8. System Updates: Agencies shall apply system updates and security patches to their systems in a timely manner. Agencies shall:
a. Establish a patch methodology
b. Test patches/updates prior to installation
c. Install critical patches for active exploits within five (5) business days of release

d. Non-critical patches shall be applied per a schedule established by the agency

9. Physical Security: Agencies shall provide appropriate physical security for their information technology systems to prevent unauthorized access.

a. Servers, routers, switches and other network equipment shall be stored securely in a locked cabinet or room

10. Security Incidents: Agencies shall notify the Information Security Office of security incidents that involve the disclosure of confidential information, unauthorized access to systems or that may affect other agencies.

a. Agencies shall develop procedures for incident response and identify an incident response team
b. Agencies shall isolate and respond to incidents originating from their systems
c. Law enforcement shall be notified when appropriate
d. DAS-ISO shall notify appropriate agency personnel of security incidents affecting their agency.

11. Security Awareness and Training: Agencies shall:

a. Provide and track security awareness training for new users upon hire and refresher training for all users on an annual basis
b. Provide and track technical security training annually for staff responsible for managing agency interconnections
c. Provide training on Enterprise Security Standards
d. Establish an acceptable use policy and distribute it to all users

12. Security Reviews: Each agency shall review their security controls at least annually, or when significant change occurs. Agency security reviews shall cover all agency systems and include the following:

a. Annual vulnerability assessment
b. Annual external penetration test including all external connections to the agency
c. Documentation of security problems
d. Develop a remediation plan to address security problems

The Information Security Office shall conduct annual security reviews of state systems.

13. Communication: Agencies shall maintain communication with the Information Security Office. Agencies shall provide the Information Security Office with:

a. The name and phone number for the:
    i. Primary security personnel
    ii. Primary technical personnel
b. A list of new, restored or terminated interconnections
c. A network diagram and list of internal and external IP addresses

14. Disconnection: Agencies are subject to emergency disconnection from the shared State IT infrastructure. Agencies may be disconnected if any of the following occur:

a. An agency system is infected by malware and remediation is unavailable
b. An agency system is infected by malware and there is a high risk of infecting other systems
c. An agency system compromise
d. Confidential information is at risk of disclosure
e. An agency system is accessed by an unauthorized user

Prior to disconnection agencies shall be:

a. Given the opportunity to isolate and investigate the incident
b. Notified by telephone and receive e-mail confirmation of the notification
c. Provided details on when and under what conditions the interconnection shall be restored
d. If an agency cannot be reached and an emergency exists item “b” may be omitted

15. Modems: Agencies shall prohibit unauthorized dial-in modem access. Modems shall:

a. Require management approval
b. Disconnect from the phone line when not in use
c. Use a callback feature where possible
d. Disable the modem answering capability if not needed

16. Intrusion Detection System: Agencies shall implement and monitor an intrusion detection system (IDS). All traffic to/from agency interconnections shall be monitored.

Effective Date
Agencies must be fully compliant with this standard on or before June 22, 2011.

Enforcement
This standard will be enforced pursuant to Iowa Administrative Code 11—25.11(8A).

Variance Iowa Administrative Code 11 - 25.11(2) provides for variances from security standards. Requests for a variance from any of the requirements of this policy will be submitted in writing to the Chief Information Security Officer prior to implementation.