Iowa Department of Administrative Services

Chester J. Culver, Governor
Patty Judge, Lt. Governor

Mollie K. Anderson, Director

State of Iowa Enterprise Information Security Standard

3-18-2008

Purpose

This Standard establishes the minimum computer security requirements for state agencies with the goal of protecting the confidentiality, integrity and availability of state computing systems and information.

Overview

State agencies collect and process a variety of information, including confidential information, in the course of their activities. Measures must be taken to protect agency information and the supporting computer systems from unauthorized access, modification, destruction, whether accidental or intentional, and to ensure authenticity, integrity and availability of state computer systems and information.

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 an agency. Information technology assets covered by this policy include those that process, store, transmit or monitor digital information. It includes the security of information technology facilities and off-site information storage; computing, telecommunications and applications related services purchased from other state agencies or commercial entities; and Internet-related applications and connectivity.

This policy 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 security standards, as well as participate in enterprise level security programs.

Updates

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

DEFINITIONS

Selected terms used in the Enterpise Security Standard are defined below:

- **Confidentiality** - The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.
- **Integrity** - The property that sensitive information has not been modified or deleted in an unauthorized and undetected manner.
- **Availability** - Ensuring timely and reliable access to and use of information.

ENTERPRISE INFORMATION SECURITY STANDARD

It is the Information Security Standard of the State of Iowa that:

1. Trusted Environment: Each agency operates in a manner consistent with the maintenance of a shared, trusted environment within state government. Agencies shall not jeopardize the confidentiality, integrity or availability of state computing systems; or the information stored, processed and transmitted by any state information system.

2. Enterprise Standards: Each agency follows established enterprise security standards except where agency policy provides a higher level of security.

3. Policy: Each agency is responsible for developing policies, processes and procedures to meet this standard. Agency policies may be more stringent than the Enterprise standard. All employees, including interns, contractors, temporary and part-time employees, must agree (in writing or electronically) to follow state and agency security policies before being authorized to access state computer resources.

4. Continuity Plan: Each agency will develop, implement, and exercise an agency business continuity plan. The plan will be based on asset criticality and be consistent with the enterprise continuity of operations plan.

5. Training: Each agency will implement a security awareness/training program for all staff. New employees will be provided basic information technology security training within three months of employment. Additional training, commensurate with the employee's work duties, will be provided annually.

6. Audits: Each agency is subject to a periodic security audit to ensure compliance with this and other enterprise level policies, standards, processes and procedures. An audit or review performed under another authority, such as the Internal Revenue Service, may be substituted if similar in scope and approved by the Chief Information Security Officer.

7. Vulnerability Assessment: Each agency will have a vulnerability assessment performed on its information systems at least annually to gauge the effectiveness of security measures. Assessment results shall be used to help identify, prioritize, plan for and implement additional security measures.

8. Risk Assessment: Each agency will have an information systems risk assessment performed at least every two years. This assessment will be used to help identify, prioritize, plan for and implement additional security measures. The assessment methodology will be developed by the Information Security Office and made available to the enterprise.

9. System Development Life Cycle: Security requirements will be formally defined and addressed throughout the life cycle of all information technology projects, including business requirements definition, design, development, testing, implementation and operation.

10. Agency Compliance: Each agency Chief Information Officer will assure to the best of his or her ability that information systems under their control meet enterprise and agency security policies, standards, processes and procedures prior to being placed in production or after significant changes to the system. The Information Security Office may randomly assess the self-certification process and individual systems to ensure adherence to policy.

11. Privacy: Confidential information that could affect individual privacy will be protected at all times.

12. Monitoring: Monitoring of information system usage for malicious activity and misuse of government resources will be conducted by agencies, or by the Department of Administrative Services, the Iowa Communications Network or other party at the request of the agency.

13. Incidents: Agencies shall report information security incidents that impact, or have the potential to impact, state shared resources to the Information Security Office following a common response plan.

14. Physical Protection: Agencies shall ensure that computer resources and physical information, including but not limited to servers, desktops, laptops, network equipment, firewalls, hardcopies and tapes, have appropriate physical protections in place. Where possible, these resources should also be protected from structural and environmental threats.

15. Network Connections: Agencies will provide information to the Information Security Office describing all connections from their agency networks to outside resources including the Department of Administrative Services shared campus network, the Iowa Communications Network, private service providers, federal, local and municipal governments and other state agencies. Updates will be provided as changes occur.

16. System Updates: Agencies will develop procedures for implementing timely system patches, configuration updates, and other measures necessary to protect systems. The procedures will provide for adequate testing prior to implementation.

17. Security Program: Agencies shall designate a person(s) responsible for coordinating the information technology security functions within the agency and for implementing the agency's information technology security policies.

18. Metrics: Agencies shall develop metrics to be used in measuring the effectiveness of their information security program, standards and practices. The DAS Information Security Office will provide assistance to agencies in developing metrics.

19. Variances: Requests for a variance from any of the requirements of this policy will be submitted in writing by the agency director to the Chief Information Security Officer prior to implementation.

Effective Date
This standard shall be effective June 30, 2008.

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