State of Iowa Enterprise Information Security Compliance Standard

December 2, 2009

Purpose

This standard establishes information security compliance reporting requirements for participating State of Iowa Agencies. The reports will update the Technology Governance Board on the current status of agency compliance with security standards and ongoing efforts to reduce risk.

Overview

As provided for under Iowa Code section 8A.204, the Technology Governance Board, in conjunction with the Department of Administrative Services, develops and adopts information technology standards pursuant to section 8A.206. These enterprise information security standards help protect the confidentiality, integrity and availability of state computing systems and information. Each agency director is ultimately responsible for ensuring that their agency complies with the enterprise information security standards. This standard establishes the requirement for agency reporting to the Technology Governance Board.

Scope

This standard applies to all participating agencies as defined by Iowa Code Chapter 8A.201. Non-participating agencies are encouraged to follow this and other enterprise level standards, policies, guidelines, processes and procedures.

Definitions

Selected terms used in the standard are defined below:

- **Enterprise Information Security Standards:** Information Security Standards developed and adopted by the Technology Governance Board (TGB) per IAC 11 - 25.9. The standards are located on the DAS Information Technology Enterprise website at:

  http://das.ite.iowa.gov/standards/enterprise_it/index.html

  under Chapter 12 - IT Security.

Updates

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

Enterprise Information Security Compliance Standard

1. **Compliance.** Agencies shall comply with all State of Iowa enterprise information security standards. To comply, an agency must meet the requirement or have been granted a variance in accordance with IAC 11—25.11.

2. **Reporting.** Agency directors shall report annually, on a form provided by the Technology Governance Board, that they are in compliance with all State of Iowa enterprise information security standards in effect at the time of the reporting. The Agency reporting form must be completed, signed and submitted to the Technology Governance Board annually by March 15.

3. **Remediation**. Agencies not compliant with the enterprise information security standards shall submit a remediation plan to the Technology Governance Board annually by March 15. The remediation plan shall identify non-compliant components and a timeline for achieving compliance.

4. **Verification**: The DAS Information Security Office (ISO) shall conduct periodic assessments to verify that agencies are in compliance with enterprise information security standards. Assessment results will be reported to the Technology Governance Board and the ISO will recommend actions to address non-compliance.

Effective Date This standard shall be effective September 1, 2010.

Enforcement This standard shall be enforced by the Technology Governance Board.

Variance Requests for a variance from any of the requirements of this standard will be submitted in writing to the Technology Governance Board.