State of Iowa Enterprise Data Stewardship Security Standard

September 2, 2014

Purpose

This Standard establishes the data stewardship requirements for state agencies with the goal of protecting the confidentiality, integrity and availability of state data.

Overview

State agencies collect and process a variety of data, including confidential information. Measures must be taken to protect data from unauthorized modification, destruction or disclosure, whether accidental or intentional, and to ensure its authenticity, integrity and availability.

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. Data includes any information both electronic and in paper format that is processed, stored or transmitted by a state agency.

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 policies, standards, processes and procedures, as well as participate in enterprise level security programs.

DEFINITIONS

Selected terms used in the Enterprise Data Stewardship Standard are defined below:

- **Availability** - Ensuring timely and reliable access to and use of information.
- **Confidential Data** – Data identified as confidential according to the agency's data classification policy.
- **Confidentiality** - The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.
- **Data Breach** – A data breach is the unauthorized (intentional or unintentional) exposure, disclosure, or loss of personal or financial information.
- **Data Steward** – Individuals with planning and policy level responsibility for data within the agency. Data stewards have the responsibility of ensuring that the appropriate steps are taken to protect the data and that respective policies and guidelines are being properly implemented.
- **Integrity** - The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Elements
The following are the elements of the Enterprise Data Stewardship Security Standard.

1. **Data Steward(s)**: Each agency shall designate a data steward(s) responsible for maintaining the accuracy, privacy, and security of the data collected by the agency.

2. **Necessity**: Agencies shall only collect confidential data necessary for meeting the agency's mission and legal requirements.

3. **Retention**: Agencies shall only retain confidential data necessary for meeting the agency's mission and legal requirements.

4. **Access**: Agency's shall ensure that only authorized users access confidential agency information. Authorized users are those with a legitimate and necessary business need to the data.

5. **Storage**: Confidential data shall be securely stored. Electronic data should be stored on a centrally managed server if possible. Confidential data transmitted or stored outside of agency control shall adhere to the requirements of Standard 10 below.

6. **Transmission**: Confidential data shall be transmitted securely.

7. **Training**: Agency security awareness training shall include a section on protection of confidential information.
    a. Organizations\individuals (i.e. county treasurers, attorneys, auditors) that have been granted access to confidential state data\systems shall receive security awareness training prior to receiving access.

8. **New System Development**: Agencies are discouraged from using confidential data to test computer systems in development. If confidential data must be used for testing, the development system shall meet the same security standards as the production system.

9. **Social Security Numbers**: Collection and use of social security numbers shall be limited and based on a strong business need. Social Security numbers shall not be:
    a. Used as a unique customer number.
    b. Used as the primary key in databases except where required by law.
    c. Displayed in full on external web-based applications beyond the initial data entry screen.
    d. Displayed in full on printed materials.

10. **Encryption**: Database fields containing confidential information shall be encrypted at rest using AES (256 bit) or stronger encryption.

11. **Data Sharing**: Sharing of confidential information outside of the agency shall be kept to a minimum. Agencies shall:
    a. Have a written policy covering data sharing.
    b. Require a signed, written data sharing agreement between the agency and outside entity prior to the exchange of data. The agreement shall include:
        i. The data to be shared;
        ii. The intended use of the data;
        iii. The time period covering the exchange;
        iv. The requirement that the requestor will protect the confidentiality of the data;
        v. The requirement that the requestor will not re-disclose the data;
        vi. The requirement that the requestor will report lost or stolen data immediately to the agency; and
        vii. Provisions for final disposal of the data.
    c. Maintain a record of data sharing agreements.
    d. Encrypt electronic data prior to transmitting.
    e. Ensure that data sharing is compliant with state and federal laws.

12. **Data Publication**: Agencies shall use comprehensive disclosure avoidance techniques consistent with professionally acceptable standards to de-identify confidential data before releasing it to the public.

13. **Disposal**:
    a. Devices and media containing confidential data shall be erased with a DoD approved method prior to disposal. Devices that cannot be wiped shall be shredded.
    b. Paper documents containing confidential data shall be shredded using a micro-cut shredder before disposal or delivery to a recycler.

14. **Notification**: State agencies shall notify individuals affected by a data breach. Notice shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach of security and with the legitimate needs of law enforcement.

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

Effective Date This standard shall be effective September 2, 2014.

Enforcement This standard shall 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. http://das.ite.iowa.gov/standards/waiver.html