DAS

Iowa Department of Administrative Services

Government's Partner in Achieving Results

Governor Terry E. Branstad
Lt. Governor Kim Reynolds

Mike Carroll, Director

State of Iowa Enterprise Email
Security Standard

December 14, 2011

Purpose

This standard establishes the minimum requirements for securing information sent via email.

Overview

State agencies rely on email to communicate with customers. The state sends and receives millions of email messages daily. Unencrypted email does not provide a secure method for transmitting confidential information. Confidential information sent via plain text email has the potential to be read by unauthorized individuals.

Scope

This standard sets the minimum requirements for the secure use of email to transmit confidential information.

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

- **Confidential Information**: Confidential information includes:

  1. Personal information defined by Iowa Code 715c. Personal information includes an individual's first name/initial and last name in combination with one, or more, of the following:
     a. Social security number.
     b. Driver's license number.
     c. Unique identification number. Ex. Iowa Student State ID; Medicaid ID.
     c. Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password.
     d. Unique electronic identifier or routing code, in combination with any required security code, access code, or password.
     e. Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

  2. Any information or record deemed confidential under Section 22.7 of Iowa Code Chapter 22, also known as the Iowa Open Records Law.

  3. All protected health information for agencies covered by the Health Insurance Portability and Accountability Act (HIPAA).

4. All protected credit card information as defined by the Payment Card Industry – Data Security Standard (PCI-DSS).

5. Any other information that if lost, disclosed, corrupted, or accessed by unauthorized means would violate state or federal law.

6. All information defined as confidential by contact/agreement with agency trading partners, customers, vendors or other entities.

- **Personal Email Accounts:** Email accounts not provided by a state agency (i.e. accounts other than user@iowa.gov or user@agency.state.ia.us).

Updates

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

Enterprise Email Security Standard

1. **Confidential Information**: Outbound agency email shall be scanned for confidential information. Email with confidential information, sent by unauthorized personnel, shall be blocked from being sent.

2. **Encryption**: All agency email messages with confidential information, either in the body or as an attachment, shall be encrypted.

3. **Federal Tax Information (FTI)**: Federal tax information shall not be transmitted via email.

4. **Credit Card Information:** Unencrypted primary account numbers (PANs) shall not be sent via email.

5. **Personal Email Accounts**: Confidential agency information shall not be transmitted using personal email accounts.

6. **Client Security**: The following shall be implemented on email clients:
   a. Disable automatic opening of messages.
   b. Disable automatic loading of pictures in messages.
   c. Disable automatic downloading and processing of active content.

7. **Training**: Agency employees, contractors, interns, and volunteers shall receive annual training on secure email practices.

8. **Customer Email:** Agencies shall instruct customers not to send confidential information to the agency via unencrypted email.

Effective Date This standard shall be effective December 14, 2011.

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.