State of Iowa Enterprise Telework Security Standard

December 14, 2011

Purpose

This standard establishes the minimum security requirements for teleworking by state employees, contractors, volunteers, and interns.

Overview

Many state agencies provide staff with the option to work from an alternate work site including their home. The security risk associated with unmanaged telework arrangements can be costly and impact the ability to deliver essential public services. Agencies must understand the risk associated with teleworking and implement measures to offset those risks.

Key to establishing a secure telework arrangement is addressing the security of information while:

- **At rest**: Data stored on a telework device such as laptop, desktop or removable storage device.
- **In transit**: Data traveling between the agency and the telework location; and
- **In use**: Data being used by the telework employee.

Agency telework equipment and information must have the same, or greater, protections than those implemented at the agency's main location.

Scope

This standard sets the minimum requirements for secure teleworking. 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

- **Cloud-Based Applications**: Applications delivered via the Internet, such as Google Docs, rather than installed on the user's computer.

- **Multi-homed connection:** A computer connected to two or more networks or having two or more network addresses. For example, a computer may be connected to a serial line and a LAN or to multiple LANs.

- **Peer-to-Peer (P2P):** Peer-to-peer (P2P) file-sharing (ex. BitTorrent) allows users to share files online through an informal network of computers running the same software. Improper

configuration of file sharing may facilitate data leakage.

- **Remote Connection:** The connection of an information asset at a non-agency location to an information asset on the agency's network.

- **Split Tunneling:** The process of allowing a remote VPN user to access a public network, most commonly the Internet, at the same time that the user is allowed to access resources on the VPN. A disadvantage of this method is that it renders the VPN vulnerable to attack as it is accessible through the public, non-secure network.

- **Telework**: A management approved arrangement, covered by a telework agreement, in which a staff person regularly performs officially assigned duties at a non-agency work site including work from home.

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

Enterprise Telework Security Standard

The following elements apply to telework:

1. **Policy**: Agencies shall develop a telework security policy and share it with staff.

2. **Remote Connections**: The following apply to remote telework connections:
    a. Connections must be encrypted.
    b. Connections must use two factor authentication. Forms of two factor authentication include:
        i. User ID & Password + Certificate
        ii. User ID & Password + Token Generator
        iii. User ID & Password + Token Generator + Certificate
    c. The telework user shall not initiate two simultaneous connections to different networks (i.e., no split tunneling and no multi-homed connections).

3. **User Accounts**:
    a. Telework user accounts shall have limited privileges. Administrative privileges shall only be granted to staff with a business need for such access.
    b. Passwords for telework accounts shall not be stored with the device/equipment.

4. **Firewall**: A firewall shall be implemented at the telework location which provides inbound and outbound filtering.

5. **Document-sharing**:
    a. Use of cloud based applications must be approved by agency management.
    b. Confidential state data shall be encrypted in transit and at rest when using cloud-based applications.
    c. Peer to peer file sharing applications shall not be installed on agency computers.

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

7. **Equipment:** The following apply to equipment used to telework:
    a. Personally owned computers, removable media and other devices shall not be used for telework
    b. Agency telework equipment shall not be used for personal activities.
    c. Electronic equipment containing confidential information shall be secured when not in use.
    d. Telework desktops storing confidential information shall be encrypted.
    e. Unused applications shall be uninstalled from telework devices.
    f. Non-functioning electronic equipment shall be returned to the agency for disposal.
    g. Telework equipment shall be audited quarterly to ensure that security settings have not been disabled/altered.
    h. An inactivity timeout of 15 minutes shall be implemented on all telework laptops & desktops.
    i. Only agency approved software may be installed on agency equipment.

8. **Backups**: Electronic information used at a telework location shall be backed-up to the agency's main network storage.

9. **Security Updates**: Laptops, desktops and other mobile devices used for telework must have critical security updates for active exploits installed within 5 days of release.

10. **Hard Copy Information**:
    a. Paper documents containing confidential agency information shall be secured when not in use (i.e. placed in a locked desk or cabinet).
    b. Paper documents with confidential information shall be shredded using a micro-cut shredder if disposed of at the telework location.
    c. Agencies shall track removal and return of confidential materials, such as personnel records, to telework locations.

11. **Training**: Agency employees, contractors, interns and volunteers shall receive training on secure telework practices prior to beginning to telework.

12. **Monitoring**: All telework remote access shall be logged and monitored. Log files shall capture sufficient detail to allow a virtual reconstruction of the network session.

13. **Reporting**: Staff shall report any security incident involving the theft/loss of equipment or unauthorized disclosure of information to the employee's supervisor within 24 hours.

14. **Wireless**: Telework wireless devices shall be configured so that they do not automatically attempt to join wireless networks they detect.

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.