Effective Date: 9/1/17

Mobile Device Security Standard

Purpose

The Mobile Device Security Standard provides documentation of the security requirements for use of laptop computers and mobile device(s) (e.g. tablet, cell phone, PDA, smart watch or smart eyeglasses, etc.) to access confidential or restricted data.

Standard

Laptops and mobile devices are required to meet the following DOA/DET policies and standards:

- Access Control Policy and Standard
- Appropriate Use of Software Standard
- Configuration Management Policy and Standard
- Media Protection Policy and Standard
- System and Communications Protection Policy and Standard
- Wireless Access Standard

In addition, the following security requirements must be met:

- Laptops that store confidential data must have full disc encryption
- Mobile devices that access confidential data must not store the data
- Mobile Device Management (specific to mobile devices only)
    - Mobile device management controls must be in place that include security policies, procedures, inventory, and standardized security configurations (including anti-malware and remote wipe features) for all devices (AC-19, MP-6);
    - Protection mechanisms must be in place in case a mobile device is lost or stolen including remote wipe features and all data stored on the device must be encrypted, including internal storage and removable media storage, such as Micro Secure Digital (SD) cards (MP-6, SC-13, SC-28);
    - Information on mobile devices must be removed (wiped) or rendered inaccessible from mobile devices after five consecutive incorrect authentication attempts, regardless of time between incorrect attempts (AC-7);
    - A centralized mobile device management solution must be used to manage agency-issued and personally-owned mobile devices prior to allowing access to the internal network (AC-3); and,
    - Information on mobile devices must be removed (wiped) or rendered inaccessible from mobile devices after five consecutive incorrect authentication attempts, regardless of time between incorrect attempts (AC-7).

Effective Date: 9/1/17

Definitions

- Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.
- DET/State information - Any information that is created, accessed, used, stored, or transmitted by an Agency and/or DET.
- DET/State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to; network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by DET.

Compliance References

IRS Pub. 1075
NIST 800-53 Revision 4

Exception Process

Exceptions to this and all DET Security policies or procedures must follow the DET Exception Procedure.

Document History/Owner

This standard was developed as required by the Department of Administration, DET Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Effective Date: 9/1/17

Version	Approval/Revision/Review Date	Description	Approver/Author, Title
.1	7/12/2016	Original	Tanya Choice Cybersecurity Compliance Consultant
1.0	8/28/17	Final Approval	Bill Nash CISO

Authorized and Approved by:

Bill Nash	Bill Nash	8/28/17
Print/Type	Signature	Date

Division of Enterprise Technology-Bureau of Security

Chief Information Security Officer