Mobile Device Usage Policy & Security Standard Background

Replaces IT Security Standard 141.10 (3.1.7, 5.2.4, 5.8) and Mobile Device Usage 191

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

Most of the original standard is the same. Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.

- Updates to this standard draws from SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices in the Enterprise
- Laptops and non-agency devices are now addressed by the policy.
- Requirements to communicate agency mobile device policies were updated include timing: onboarding, annually, and when revised.

What is the business case for the policy/standard?

- State agencies have an affirmative duty under state law to retain, preserve exempt and non-exempt public records, and produce non-exempt public records in response to a request, including those created, accessed, used, or stored on mobile devices.
- This standard helps agencies increase freedom of movement while conducting state business with an understanding of the risks to their IT assets, and to employ appropriate controls.

What are the key objectives of the policy/standard?

The objectives of this policy are:

- Establish policy for the roles, responsibilities, and standard practices concerning the effective and efficient management of mobile devices used to access the state IT Assets and conduct government business.
- Ensure the understanding of risk and responsibility and that it is documented and understood.
- Agencies also have a duty to preserve and produce records for litigation purposes. Public records, both exempt and non-exempt, include those records – including, but not limited to, texts, voice mail, email, instant messaging, calendars, photos, and video – an employee prepares, owns, uses, receives, or retains within the scope of employment. Agency mobile device usage policies must address and conform to these requirements.

How does policy/standard promote or support alignment with strategies?

This policy strengthens IT Architecture & Security by requiring agencies to secure assets with the portability and high risk of potential incidents. It also addresses the use of non-agency mobile devices.

What are the implementation considerations?

- Agencies will need to verify and update awareness training to include mobile device policies.
- Agencies may need additional training and support.

How will we know if the policy is successful?

- Agencies will minimize data leakage from the use of mobile technology.
- Agencies will decrease the number and severity of incidents involving mobile devices including losses and resets.

Application Security Standard Background

Replaces IT Security Standard 141.10 (7.1- 7.5)

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

Most of the application security standard is consolidated from OCIO 141.10, sections 7.1 through 7.5. New language includes references to the Security Design Review process, the Security Assessment and Authorization Standard, the Vulnerability Management Standard, and the Change Management Policy.

What is the business case for the policy/standard?

Agencies depend on software applications to deliver on many aspects of their missions. The requirements in the standard ensure that data processed by these applications is not disclosed, altered, or destroyed without authorization.

What are the key objectives of the policy/standard?

- Agencies must perform risk assessments on new applications and those which process category 3 data.
- Agencies must identify, and plan to resolve, application vulnerabilities prior to production deployment.
- Agencies must follow secure coding practices when developing any type of software application.

How does policy/standard promote or support alignment with strategies?

- Increase security capabilities to protect mission-critical systems and data.
- Align architecture with leading industry trends, standards**,** and best practices.

What are the implementation considerations?

- Agencies must document how they implement secure coding practices into their software development methodology.
- Agencies must implement software functionality and security testing tools appropriate to their software development methodology.

How will we know if the policy is successful?

Specific: Agencies will manage risks with each application processing category 3 data and higher.
Measurable: Agencies will document risk assessments, plans, and changes for applications.
Achievable: WaTech will offer templates for support.
Relevant: Application security is an essential measure to protect data.
Timely: As agencies purchase or develop applications.
Equitable: Agencies of all sizes utilize applications to operate business, and will benefit from managing the risks of each application.

WaTech
Washington Technology Solutions

Encryption Standard Background

New, Update or Sunset Review? Update.

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

In discussion with agencies, the requirement to use FIPS mode for category 3 and 4 data may cause functionality issues with some applications. We changed this requirement to apply only when necessary by federal requirements.

What is the business case for the policy/standard?

- **Encryption protects state data from exploitation by making data unreadable and unusable to unauthorized viewers.**
- Encryption confirms authenticity of the data source.

What are the key objectives of the policy/standard?

The key objective of this standard is that agencies encrypt data and storage media using industry standards.

How does policy/standard promote or support alignment with strategies?

Encryption of data stored or in transit maintains information confidentiality and integrity, including confidential information requiring special handling. Alignment with these strategies supports compliance with statutory and regulatory requirements specific to the type of information stored or transmitted.

What are the implementation considerations?

- **Agencies will need to map the risk of their data to their agencies based on classification.**
- Agencies will need to select the appropriate encryption algorithm commensurate with the risk.
- Agencies will need education and support from WaTech.

How will we know if the policy is successful?

Specific: Agencies will be able to apply encryption commensurate with the risk of the information being protected.

Measurable: The SDR workload is reduced long-term because risk assessments are performed regularly.
Achievable: Agencies will map the risk and encryption needs of the different classifications of their data.
Relevant: Encryption and protection of data is increasingly important with new developments in cyber crime.
Timebound: The standard is immediately effective.
Equitable: Encrypting data protects everyone's interests.

WaTech
Washington Technology Solutions

Security Logging Standard Background

Replaces IT Security Standard 141.10 (10)

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

Most of the original standard is the same. Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.
Updates to this standard draws from NIST Special Publication 800-92, Guide to Computer Security Log Management.

What is the business case for the policy/standard?

- Ensure agency configure their security logging to the requirements in this standard.
- Security logs are a resource for reconstructing events and business recovery activities.

What are the key objectives of the policy/standard?

- Safeguard the resources used to detect, identify, and respond to security events, policy violations, and fraudulent activity.

How does policy/standard promote or support alignment with strategies?

This standard strengthens IT Architecture and security by ensuring that agency environments, and those environments which interconnect agencies to the State Government Network, maintain records of security events that may cause harm to state resources.

What are the implementation considerations?

- Agencies may need additional training and support on security log transmittal.
- Agencies will need to review and verify their security logging procedures align with this standard.

How will we know if the policy is successful?

- WaTech enterprise Security Information Event Management (SIEM) system will indicate the transmittal of security logging data.
- Agencies will possess up-to-date procedures that reflect the requirements of this standard.

WaTech
Washington Technology Solutions

Privacy and Data Protection Background

New, Update or Sunset Review? New.

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

The content was primarily adopted from industry standard privacy frameworks. The NIST Privacy Framework is a collaborative tool intended to help organizations identify and manage privacy risk. In 2022 the Office of Privacy and Data Protection adopted the Washington Privacy Framework, which is a simplified version of the NIST Privacy Framework. It is intended to help state agencies implement effective privacy practices. The content of this policy incorporates the foundational components of the Washington Privacy Framework that are appropriate for all state agencies.

The Office of Privacy and Data Protection also considered the data collected as part of its annual privacy assessment of state agencies and consulted with the Privacy Community of Practice and State Agency Privacy Forum.

What is the business case for the policy/standard?

Although there has been significant improvement in recent years, there is still a wide range of privacy maturity across the state agency enterprise. The benefits vary depending on each agency's current maturity:

- For agencies with strong, established privacy programs the new policy will more formally create baseline components to review and iterate on.
- For agencies with relatively new or incomplete privacy programs, the policy will help identify gaps and prioritize efforts.
- For agencies with few privacy practices in place, the policy will help identify and implement foundational privacy practices.

Agencies at all levels of the maturity scale have indicated that having privacy requirements in policy would help create internal momentum for prioritizing and communicate requirements to vendors.

What are the key objectives of the policy/standard?

The policy covers a range of foundational privacy practices. Key elements include:

- Designated privacy contacts
- Policies and procedures
- Privacy threshold analyses / privacy impact assessments (PTAs/PIAs)
- Training
- Data disposal
- Privacy notices
- Individual participation
- Incident response
- Monitoring
- Biometrics

How does policy/standard promote or support alignment with strategies?

Each state agency implementing baseline privacy protections is essential to the digital trust pillar of the Enterprise IT Strategic Plan. The digital trust pillar upholds and is interwoven in all of the 2023-2025 Enterprise IT Strategic plan goals.

What are the implementation considerations?

As measured by the Office of Privacy and Data Protection's annual privacy assessment of state agencies, most components of this policy are in place at most agencies. Most components already exist in statute, executive order, or state policy. Some agencies will need to take additional steps to comply with new requirements. The Office of Privacy and Data Protection has existing resources to help with implementation.

How will we know if the policy is successful?

The state will know if this policy is successful if agencies make progress on the policy requirements. This will be measured by data collected in the state's Annual Privacy Assessment Survey which asks about the specific policy requirements. Data collected from the most recent privacy assessment surveys already indicate that the privacy policy requirements are achievable. The policy requirements are both relevant and equitable given the Washington's focus on digital equity and agencies collection and use of personal data. The year-over-year data from the annual privacy assessment and policy sunset review date will be used as the timeline for measuring policy success.