Policy & Standard Background

Name: Encryption Standard

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 2017 version of OCIO 141.10 section 4.3 describes the minimum data encryption and management requirements, and 4.4 describes minimum encryption standards during transit. This new standard builds upon this by adding requirements from NIST 800-175A, Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies, and NIST-800-57 – Recommendations for Key Management.

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 inventory category 3 and 4 data.**
- **Agencies will need to map the risk of that data to their agencies.**
- **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?

- **Agencies will be able to apply encryption commensurate with the risk of the information being protected.**
- **The SDR workload is reduced long-term because risk assessments are performed regularly.**

State CIO Adopted:
TSB Approved:
Sunset Review:

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Replaces:
IT Security Standard 141.10 (4.3 & 4.4)
December 11, 2017

ENCRYPTION STANDARD

See Also:
RCW 43.105.054 OCIO Governance
RCW 43.105.450 Office of Cybersecurity
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"

1. **Agencies must use approved standards to protect category 3 and category 4 and may use these standards for category 1 and 2 data as described in the Data Classification Standard.**
2. **Agencies must perform full disk encryption for all workstations that access or contain agency information.**
    a. Full disk encryption products must use either pre-boot authentication that utilizes the device's Trusted Platform Module (TPM), or Unified Extensible Firmware Interface (UEFI) Secure Boot.
    b. Encryption of the entire hard drive volume and all files on the hard drive must meet National Institute of Standards and Technology Federal Information Processing Standards (NIST FIPS) 140-3 Level 1 minimum requirements.
3. **Agencies must use NIST FIPS approved encryption for the confidentiality and integrity of data at rest and data in transit.**
    a. A cryptographic module does not meet the requirements or conform to the NIST FIPS standard unless a reference can be made to the validation certificate number.
    b. Use of outdated, cryptographically broken, or proprietary encryption algorithms/hashing functions is prohibited.
    c. Agencies must use FIPS mode if processing Sensitive But Unclassified data (SBU), which maps to Category 3 on the Data Classification Standard.
    d. Electronic information used to authenticate the identity of an individual or process must be encrypted when stored, transported, or transmitted.
        i. This does not include the distribution of a one-time use PIN, password, passphrase, token code, etc., provided it is not distributed along with any other authentication information
4. **Data must be encrypted at rest.**
    a. Agencies must select and apply encryption for category 3 and category 4 data using NIST FIPS 140-3 encryption algorithms in such a way that the data becomes unusable to anyone but authorized personnel.
    b. Agencies must protect the confidential process, encryption key or other means to decipher the information from unauthorized access.
5. **Agencies must use approved encryption algorithms for category 3 and category 4 data in addition to consideration for special handling requirements.**
    a. Symmetric encryption: NIST FIPS 197 validated Advanced Encryption Standard (AES) (≥ 128- bit).

b. Asymmetric encryption: RSA (≥ 2048-bit).

c. Hashing: NIST FIPS 180-4 validated SHA-2 and SHA-3

6. Data must be encrypted while in transit.

a. Agencies must appropriately protect information transmitted electronically. The transmission of category 3 and 4 data requires encryption such that:

i. All manipulations or transmissions of data during the exchange are secure.
ii. If intercepted by unauthorized parties during transmission the data cannot be deciphered.
iii. When necessary, confirmation is received when the intended recipient receives the data.

b. Appropriate encryption methods for data in transit include, but are not limited to:

i. Transport Layer Security (TLS) 1.2 or later version.
ii. Secure Shell (SSH) 2.0 or later version.

c. Clients and servers must be configured to support the strongest cipher suites possible. Ciphers that are not compliant with this standard must be disabled.

7. Agencies must protect cryptographic keys.

a. Keys must be distributed and stored securely.

b. Access to keys must be restricted to individuals who have a business need.

c. Unencrypted keys must not be stored with the data that they encrypt.

d. Encryption keys and their associated software products must be maintained for the life of the archived data that was encrypted with that product.

e. Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted. If a compromise has been discovered a new key must be generated and used to continue protection of the encrypted information. See the state Incident Response Plan and IT Policy 143 - Incident Response Communication.

REFERENCES

1. Data Classification Standard
2. Definition of Terms Used in WaTech Policies and Reports
3. IT Policy 143 - Security Incident Communication
4. Definition of Terms Used in WaTech Policies and Reports
5. NIST SP 800-175A - Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies
6. NIST SP 800-52
7. NIST SP 800-57 Part 1, Recommendation for Key Management
NIST SP 800-57 Part 2– Best Practices for Key Management
NIST SP 800-57 Part 3 Application-Specific Key Management Guidance
10. NIST FIPS 140-3
11. NIST FIPS 197
12. NIST FIPS 180-4

13. NIST Cybersecurity Framework Mapping
    - ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.
    - PR.DS-1: Data-at-rest is protected.
    - PR.DS-2: Data-in-transit is protected.
    - PR.IP-4: Backups of information are conducted, maintained, and tested.
    - PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
    - PR.AT-2: Privileged users understand their roles and responsibilities.

CONTACT INFORMATION

- For questions about this policy, please contact the WaTech Policy Mailbox.
- For technical security questions or to submit risk assessments, please contact the WaTech Risk Management Mailbox
- To request a Design Review, please contact sdr@watech.wa.gov.