

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 and laptops 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 (NIST) Federal Information Processing Standards (FIPS) [FIPS 140-3 Security Requirements for Cryptographic Modules](#) Level 1 minimum requirements.
3. **Agencies must use NIST FIPS 140-3 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 140-3 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 - b. Use of outdated, cryptographically broken, or proprietary encryption algorithms/hashing functions is prohibited.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 when required by federal partners.
 - 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 encryption algorithms from 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: [FIPS 197 - Advanced Encryption Standard \(AES\)](#) validated Advanced Encryption Standard (AES) (≥ 128 - bit).
- b. Asymmetric encryption: RSA (≥ 2048 -bit).
- c. Hashing: [FIPS 180-4 Secure Hash Standards \(SHS\)](#) 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 - Guidelines for the Selection, Configuration, and Use of Transport Layer Security \(TLS\) Implementations.](#)
7. [NIST 800-53 - Security and Privacy Controls for Info Systems and Organizations..](#)
8. [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.](#)
11. [FIPS 140-3 - Security Requirements for Cryptographic Modules.](#)
12. [FIPS 197 - Advanced Encryption Standard \(AES\).](#)
13. [FIPS 180-4 Secure Hash Standards \(SHS\).](#)
14. 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 email the [WaTech Policy Mailbox](#).
- To request a Design Review, please email the [Security Design Review Mailbox](#).