SEC-08
State CIO Adopted: February 11, 2023
TSB Approved: March 14, 2023
Sunset Review: March 14, 2023

Replaces:
IT Security Standard 141.10 (4.2)
December 11, 2017

WaTech
Washington Technology Solutions

DATA SHARING POLICY

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"
RCW 39.26.340 Data Sharing - Contractors
RCW 39.24.240 Data Sharing - Agencies
RCW 43.105.054 OCIO Governance

1. **Agencies must enter into written data sharing agreements when sharing category 3 or category 4 data outside the agency unless otherwise prescribed by law.**

    a. Sharing involves any relationship where a person or organization outside the agency receives, hosts, or has access to information, including access to systems or applications.

    b. While these steps are required for higher categorizations of data, agencies may consider following these policies for sharing category 1 or 2 data. See the Data Classification Standard.

    c. When agencies are sharing data with a vendor in connection with a service, the service agreement must include a data sharing agreement.

    d. If there is a discrepancy in the data classification between agencies, as part of the written agreement, all parties must document the classification of the data they will assign to the data and the reason for the classification.:

2. **Agencies must identify and evaluate the risks of sharing their data and must enter into a data sharing agreement that documents the relationship and includes appropriate terms to mitigate identified risks.**

3. **Data sharing agreements can take different forms but should typically include at least:**

    a. The purpose and specific authority for sharing and time period of the agreement.

    b. A description of the data, including classification.

    c. Period of agreement.

d. Authorized uses.

e. Authorized users or classes of users.

f. Protection of the data in transit if the arrangement involves transmission.

g. Secure storage for data maintained outside the agency sharing its data.

h. Data retention and disposal responsibilities and processes.

i. Backup requirements for the data if applicable.

j. Incident notification and response.

k. Monitoring and enforcement of data protection requirements specified in the agreement.

l. All parties must have a security awareness program and/or training.

m. Compliance with all relevant state security and privacy requirements associated with the data being shared.

n. Any other requirements imposed by law, regulation, contract, or policy.

REFERENCES

1. Data Classification Standard
2. Encryption Standard
3. State Agencies Records Retention Schedules
4. Media Sanitization and Disposal Standard
5. Backup and Restoration Standard
6. Security Awareness and Training Policy
7. Data Sharing Agreement Implementation Guidance
8. Risk Management Framework for Information Systems and Organizations
9. Definition of Terms Used in WaTech Policies and Reports

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- To request a Design Review, please contact the Security Design Review Mailbox.