Policy & Standard Background

Name: Data Sharing Policy

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 4.2 cites requirements for data sharing agreements. This policy builds on this section by referencing other standards which inform the data sharing agreement. This standard also requires agencies assess the risk of sharing their data with another agency or vendor.

What is the business case for the policy/standard?

OCIO 141.10 does not require that agencies assess the risk of sharing their data. This impedes implementation of controls appropriate to mitigate that risk. It also lacks references to security requirements which impact the data sharing agreement.

The new policy requires agencies to address the risk of sharing their data. It also highlights security requirements to consider when planning to share data.

What are the key objectives of the policy/standard?

- **Require that agencies assess risk around the data set being shared with an entity external to the sharing agency.**
- **Associate each element of the data sharing agreement with relevant security requirements.**

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

This policy enables agencies to identify data sharing risks and implement controls appropriate to mitigate those risks.

What are the implementation considerations?

Agencies will need guidance on scoping and executing data sharing risk assessments.

How will we know if the policy is successful?

- **Agencies perform a data sharing risk assessment prior to data sharing.**
- **Agencies implement risk mitigation controls consistent with security standards.**

State CIO Adopted:
TSB Approved:
Sunset Review:

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Replaces:
N/A

DATA SHARING POLICY

SEE ALSO: see also

RCW 43.105.450 Office of Cybersecurity
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 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.

    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. Retention link (needs updating)
4. Media Sanitization and Disposal Standard
5. Backup and Restoration Standard
6. Incident Response Program
7. Security Awareness and Training Policy
8. Data Sharing Agreement Implementation Guidance
9. Risk Management Framework for Information Systems and Organizations (RMF)
10. Definition of Terms Used in WaTech Policies and Reports

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.