DATA-03
State CIO Adopted: June 24, 2024
TSB Approved: June 24, 2024
Sunset Review: June 24, 2027

Replaces:
NEW

WaTech
Washington Technology Solutions

PRIVACY AND DATA PROTECTION POLICY

See Also:
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (23) "State agency"
RCW 42.105.369 Office of privacy and data protection
RCW 43.105.365 Accuracy, integrity, and privacy of records and information

1. **State agencies have an obligation to protect the personal information they process to provide services and perform government functions and handle that information responsibly.**

    a. Effective privacy practices and responsible information processing enable success by reducing risk and building trust.

2. **Agencies must complete the annual privacy assessment survey conducted by the Office of Privacy and Data Protection as part of the annual certification process. See Technology Policies, Standards, and Procedures (7.b.)**

    a. As part of the annual privacy assessment survey, agencies must indicate whether or not they process personal information.

3. **Agencies must designate a privacy contact.**

    a. Designating a contact ensures accountability and efficient enterprise privacy communications.

    b. The designated contact may or may not work full-time on privacy.

    c. Resources dedicated to privacy will vary between agencies based on the size of the agency and the scope and scale of personal information the agency processes.

    d. Privacy and data protection is multi-disciplinary. This means different positions and functions may implement or influence privacy practices. Specific privacy tasks will often be allocated across different functions of each agency. Examples of functions that may work on privacy include, but are not limited, to data management, public records, risk management, data governance, information technology security, legal, contracts and audit.

4. **Agencies must understand the personal information they process, as**

demonstrated by:

a. Classifying data as required by SEC-08-01-S Data Classification Standard.

b. Completing the application inventory required by MGMT-01 - Technology Portfolio Foundation and MGMT-01-01-S Technology Portfolio Foundations-Applications .

c. Inventorying public records as required by RCW 40.14.040 Records officers—Designation—Powers and duties.

d. Reviewing records collected as required by RCW 43.105.365 Accuracy, integrity, and privacy of records and information.

5. **Agencies that process personal information must establish policies and procedures consistent with the Washington State Agency Privacy Principles and other applicable laws or handling standards.**

   a. The Washington State Agency Privacy Principles and other applicable laws or handling standards must be integrated into activities and projects that involve processing personal information.

6. **Agencies must conduct Privacy Threshold Analyses (PTA) and Privacy Impact Assessments (PIA) to identify and address privacy risks and potential privacy harms when required. See RCW 43.105.369 (3). See DATA-03-01-PR Privacy Threshold Analysis During Security Design Review Procedure.**

   a. Agencies must complete a privacy threshold analysis as part of any required WaTech Security Design Review that involves processing personal information. See Security Assessment and Authorization Policy.

   b. When a PTA indicates the potential for significant privacy risks or privacy harms, as confirmed by the state Office of Privacy and Data Protection, agencies must complete a PIA.

7. **Agencies must ensure all employees receive sufficient privacy awareness training related to their roles and responsibilities and the personal information they have access to.**

   a. At a minimum, employees must receive basic privacy awareness training that addresses how to identify personal information and employee responsibilities for protecting personal information.

      i. Agencies can satisfy this requirement by using the Privacy Basics for Washington State Employees training offered by the Office of Privacy and Data Protection.

b. Basic privacy awareness training must be completed:

   i. As part of onboarding for new employees within 30 days of start date.

   ii. At least annually.

c. Additional privacy awareness training must be provided consistent with:

   i. Individual roles and responsibilities.

   ii. The scale and sensitivity of personal information the agency processes.

   iii. Other applicable handling standards for Category 3 or 4 personal information processed by the agency.

d. Agencies should promote privacy awareness through other activities, such as participation in the annual data privacy day.

8. **Agencies must enter into written data sharing agreements when sharing category 3 or category 4 data outside the agency unless otherwise prescribed by law. See SEC-08, Data Sharing Policy; RCW 39.26.340 Data-sharing agreements—When required; RCW 39.24.240 Data requests—When written agreement required.**

   a. Agencies must send notice to the state Office of Privacy and Data Protection at privacy@watech.wa.gov prior to the sale of any personal information to third parties. See Executive Order 16-01.

   b. Section 8.a does not apply to information that has already been made available to the public.

9. **Agencies must dispose of personal information when it has met its record retention requirements and is no longer needed for the purpose it was originally collected or to comply with other legal requirements. See SEC-04-02-S Media Sanitization and Disposal Standard; Executive Order 16-01 Privacy Protection and Transparency in State Government "Modernizing State Agency Privacy Protection"; RCW 40.14.060 Destruction, Disposition of official public records or office files and memoranda – Record retention schedules; RCW 40.14.040 Records officers – Designation – Powers and duties.**

10. **Agencies must be transparent about how they process personal information by publishing privacy notices. See Executive Order 16-01.**

    a. Privacy notices must describe at least:

i. The types of personal information the agency processes.

ii. How and why the agency processes personal information.

iii. Who the agency shares personal information with, if applicable.

iv. How individuals can exercise any applicable rights to access or control their personal information.

v. How to contact the agency.

b. Privacy notices must be posted on each agency's website and may be provided via other delivery methods consistent with how the agency interacts with individuals.

c. Privacy notices must be routinely reviewed and updated to match current processing activities.

11. Agencies that process personal information must allow individuals to access or control their information to the extent consistent with applicable law and the government functions the agency performs.

a. Agencies must develop procedures to receive and respond to individuals' requests to access or correct their information.

b. Agencies should allow individuals to opt-out of or restrict processing activities when feasible or otherwise required by law.

12. Agencies that process personal information must implement adequate controls, including policies and training, to identify, report and respond to privacy incidents.

a. A privacy incident occurs when there is a potential unauthorized use or disclosure of personal information, regardless of whether the incident rises to the level of requiring breach notification.

b. Privacy incidents include any potential unauthorized use or disclosure, even if it is not an IT security incident that poses a threat to the confidentiality, integrity or availability of an IT system.

13. Agencies that process personal information must monitor and review privacy and data handling practices. This may include, establishing processes to measure privacy practices effectiveness, monitoring compliance with established policies and processes, and routinely reviewing changes in collection, use and disclosure, technology, and applicable handling requirements.

14. **Each agency using or intending to develop, procure or use a facial recognition service, or otherwise collect, capture, purchase or obtain a biometric identifier must adhere to applicable procedures and handling requirements in Chapter 43.386 RCW Facial Recognition, Chapter 40.26 40.26 RCW Biometric Identifiers and Washington state policies.**

REFERENCES

1. Technology Policies, Standards, and Procedures (7.b).
2. SEC-08-01-S Data Classification Standard.
3. MGMT-01 - Technology Portfolio Foundation.
4. MGMT-01-01-S Technology Portfolio Foundations-Applications.
5. RCW 40.14.040 Records officers—Designation—Powers and duties.
6. RCW 43.105.365 Accuracy, integrity, and privacy of records and information.
7. Washington State Agency Privacy Principles.
8. DATA-03-01-PR Privacy Threshold Analysis During Security Design Review Procedure.
9. RCW 43.105.369 Office of privacy and data protection.
10. SEC-08, Data Sharing Policy.
11. RCW 39.26.340 Data-sharing agreements—When required.
12. RCW 39.34.240 Data requests—When written agreement required.
13. RCW 40.14.060 Destruction, disposition of official public records or office files and memoranda – Record retention schedules.
14. SEC-04-02-S, Media Sanitization and Disposal Standard.
15. Executive Order 16-01 Privacy Protection and Transparency in State Government "Modernizing State Agency Privacy Protection."
16. Chapter 43.386 RCW: Facial Recognition.
17. Chapter 40.26 RCW: Biometric Identifiers.
18. Definition of Terms Used in WaTech Policies and Reports.

CONTACT INFORMATION

- For questions about this policy, please email the policy mailbox.
- For questions about privacy, please email privacy@watech.wa.gov.