Replaces:
NEW

WaTech
Washington Technology Solutions

WaTech Privacy Policy

See Also:
RCW 42.105.369 Office of privacy and data protection

1. **WaTech must protect personal information it processes to provide services, perform government functions, and handle information responsibly. To maintain public trust, safeguard sensitive information and comply with regulations WaTech must adhere to the established privacy principles articulated by the Office of Privacy and Data Protection. See RCW 43.105.369(3)(c).**

2. **WaTech must complete the privacy assessment survey required under the annual certification process. See Technology Policies, Standards, and Procedures (7.b.)**

    a. The WaTech Privacy Officer must complete the annual privacy assessment survey.

    b. As part of the annual privacy assessment survey process, the WaTech Privacy Officer must review and inventory the personally identifiable information (PII) it processes and the correlating privacy practices.

    c. The WaTech Privacy Officer will consult and collaborate with other WaTech teams as needed to complete the annual privacy assessment survey.

3. **WaTech designates the WaTech Privacy Officer as its privacy contact.**

    a. The WaTech Privacy Officer is the official contact for privacy matters specific to WaTech agency business.

    b. The State Chief Privacy Officer is the contact for privacy matters that have external or state-wide impacts.

4. **WaTech must understand the personal information it processes. This work will be completed by the WaTech Privacy Officer in coordination with other relevant WaTech Teams including but not limited to the Office of Cybersecurity, Strategy and Management, Architecture and Innovation, and the Records Management Unit.**

    a. WaTech will classify data into categories based on its sensitivity and handling requirements.

    b. WaTech will complete the application inventory as required by MGMT-01

Technology Portfolio Foundation and MGMT-01-01-S Technology Portfolio Foundations-Applications.

c. WaTech will complete and maintain an up-to-date data inventory.

d. WaTech will review records collected that concern individuals and will be widely accessible to the public as required by RCW 43.105.365 to ensure the accuracy, integrity, and privacy of the information.

5. WaTech's procedures must be consistent with the Washington State 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.

b. The WaTech Privacy Officer must be notified of and participate in review and implementation of WaTech projects involving personal information.

c. The WaTech Privacy Officer must be engaged in the WaTech Service Catalog Process regarding all new and modified services that are added to WaTech that involve personal information.

d. The WaTech Privacy Officer will review all Terms of Service for new or modified services that involve personal information.

e. The WaTech Privacy Officer will review and update the internal and external WaTech Service Action Plan for privacy annually.

f. The WaTech Privacy Officer works with Office of Cybersecurity Security Design Review (SDR) team on projects processing personal information. This includes meeting regularly with SDR team members.

g. The WaTech Privacy Officer attends all-staff meetings and extended executive team meetings to provide updates and inform internal customers on emerging projects, initiatives, and services.

h. The WaTech Privacy Officer must engage with the Privacy Community of Practice.

i. The WaTech Privacy Officer will present updates as needed to the Quarterly State Agency Privacy Form.

6. WaTech 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).

a. The WaTech Privacy Office must complete a privacy threshold analysis within 10 days in accordance with the Enterprise PTA procedure for projects that involve processing personal information.

b. When a PTA indicates the potential for significant privacy risks or privacy harms, as confirmed by the Office of Privacy and Data Protection, The WaTech Privacy Officer must complete a Privacy Impact Assessment (PIA) in coordination with other WaTech teams.

c. The WaTech Privacy Officer will oversee the implementation and execution of privacy risk mitigation controls identified in the PIA.

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

a. All Employees must complete privacy training:

i. Within 30 days of hire date.

ii. Following the initial training, employees must complete refresher training on an annual basis.

b. Additional privacy awareness training must be provided by the WaTech Privacy Officer consistent with:

i. Individual roles and responsibilities.

ii. The scale and sensitivity of personal information WaTech processes.

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

c. The WaTech Privacy Officer will further promote privacy awareness at WaTech by:

i. Participating in the annual Data Privacy Day activities.

ii. Creating informative Privacy Minute videos that raise awareness on privacy related topics.

iii. Develop interactive games focused on privacy topics to enhance privacy awareness and provide educational opportunities.

iv. Incorporating awareness of privacy into projects.

8. WaTech will exercise due diligence before and after entering into written data

sharing agreements.

a. WaTech will notify the 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. The WaTech Primary Services Agreement (PSA) and Terms of Service will comply with the WaTech Data Sharing Policy (SEC-08) and RCW 39.34.240(1).

c. WaTech contracts that share data with external partners will comply with the WaTech Data Sharing Policy (SEC-08) and RCW 39.26.340(1).

9. WaTech will only collect the minimum amount of personal information needed to accomplish a specific purpose. WaTech will dispose of personal information when it meets its record retention requirement.

a. WaTech will only collect and use personal information with appropriate legal authority.

b. WaTech will adhere to all applicable privacy laws, policies, and procedures regarding the collection of personal information.

c. WaTech will consider the potential privacy impacts of collecting or maintaining the information throughout the data lifecycle.

10. WaTech is required to have a privacy notice regarding how it collects, uses, and disposes of personal information.

a. WaTech's privacy notices must include:

i. What kind of personal information is collected by the agency.

ii. How and why WaTech processes personal information.

iii. Who WaTech shares personal information with.

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

v. How to contact WaTech regarding personal information.

b. Privacy notices will be posted on WaTech's website.

c. Privacy notices will be reviewed annually by the WaTech Privacy Officer.

11. WaTech will allow individuals to access or control their personal information to

the extent consistent with applicable law and the government functions the agency performs and allow individuals to:

a. Provide, revoke, or manage consent.

b. Opt-Out or restrict collection or use.

c. Request corrections to inaccurate information.

12. WaTech will implement appropriate safeguards to limit incidents of unauthorized access or unauthorized use of personal information. WaTech will follow the WaTech Incident Response Plan and work with the agency CISO when an incident occurs. Should an incident occur, WaTech will follow the following internal plans and procedures:

a. WaTech Security Incident Response Plan v3.1.

b. WaTech Policy 6.3.2 – Notice of Security Breach and Unauthorized Acquisition of Personal Information

c. IT Security Incident Communication.

d. Use the Data Breach Assessment Form to determine whether an incident is a breach that requires notification under RCW 42.56.590.

13. WaTech will monitor and review privacy and data handling practices whenever personal information is processed. This includes, establishing processes measuring privacy practice effectiveness, monitoring compliance with established policies and processes, and routinely reviewing changes in collection, use and disclosure, technology, and applicable handling requirements. Examples include:

a. Monitoring compliance with data sharing agreements.

b. Reviewing the WaTech privacy notice at least annually.

c. Measuring compliance with training requirements.

d. Updating the WaTech Service Action Plan

e. Keeping data inventory current.

f. Tracking incident reporting and resolution.

14. WaTech will adhere to Chapter 43.386 RCW Facial Recognition, Chapter 40.26.020 RCW Biometric Identifiers and other applicable Washington state policies when it uses facial recognition technology.

REFERENCES

1. Technology Policies, Standards, and Procedures (7.b.)
2. MGMT-01 Technology Portfolio Foundation
3. MGMT-01-01-S Technology Portfolio Foundations-Applications
4. RCW 43.105.365 Accuracy, integrity, and privacy of records and information
5. Washington State Agency Privacy Principles
6. RCW 43.105.369 (3)
7. Executive Order 16-01
8. WaTech Policy 6.3.2 – Notice of Security Breach and Unauthorized Acquisition of Personal Information
9. Data Breach Assessment Form
10. RCW 42.56.590
11. Chapter 43.386 RCW Facial Recognition
12. Chapter 40.26.020 RCW Biometric Identifiers

CONTACT INFORMATION

- For questions about privacy, please email privacy@watech.wa.gov.

DEFINITIONS

Data sharing agreement – A document that memorializes what data is being shared and how it can be used (i.e., a contract, service level agreement, or dedicated data sharing agreement).

Incident – An event with the potential to compromise the confidentiality, integrity, or availability of an organization or its information assets.

Personal Information – Information that is identifiable, directly or indirectly, to a specific individual.

Privacy Notice – A comprehensive notice that explains how an agency collects, uses, shares, and manages personal information.

Process - Operation or set of operations performed upon personal information that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer and disposal of personal information.

Safeguard – A mechanism (software, hardware, configuration, etc.) that protects something, such as information.

Third party – Anyone external to the agency such as contractors, vendors, and other state agencies, local government, researchers, and non-profit organizations.