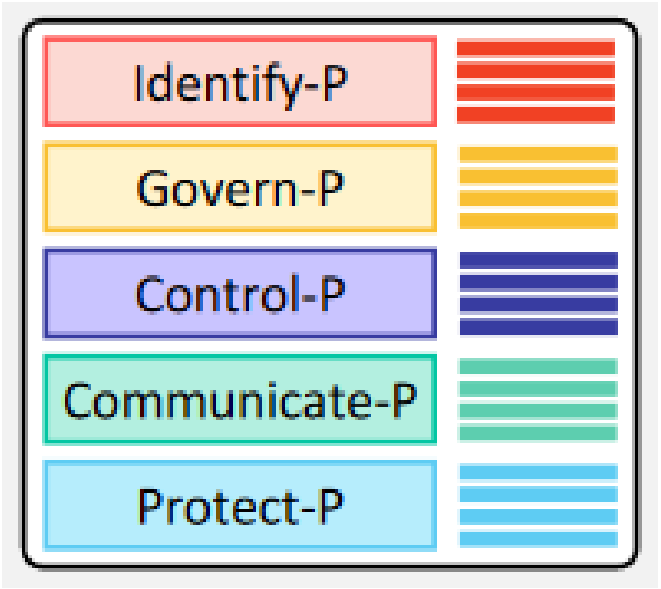
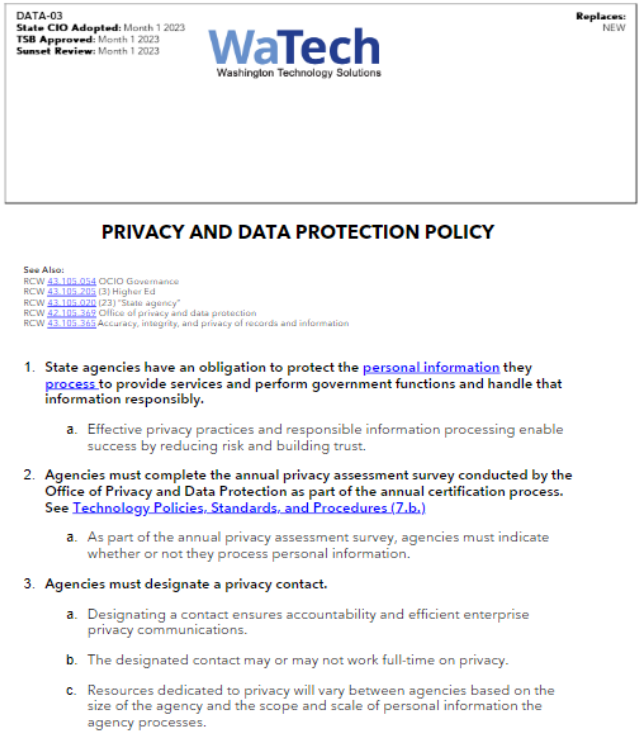
WaTech
Washington Technology Solutions

Washington State Privacy and Data Protection Policy

Requirements, guidance and suggestions





DATA-03
State CIO Adopted: Month 1 2023
TSB Approved: Month 1 2023
Sunset Review: Month 1 2023

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.

What's in it?

- 14 sections
- Reinforces existing legal requirements and existing practices
- Many sections are supported by existing OPDP resources
- Includes functional needs (not technical)

WaTech
Washington Technology Solutions

But first . . . definitions

Personal information

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

Personal information – key concepts

- Not limited to Category 3 or 4 information
- Broader than definition in RCW 42.56.590
- Can include information without direct identifiers

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.

Process – key concepts

- Any action involving personal information
- Broader than storing or maintaining

WaTech
Washington Technology Solutions

To the requirements

Section 1 – Statement of agency responsibility

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**.

Section 2 – Annual privacy assessment

Highlights

- Agencies must complete privacy assessment as part of annual certification process
- Whether an agency processes personal information controls which policy requirements apply

Resources

2020-2024 Privacy Assessment Reports

Section 3 – Privacy contacts

Highlights

- "Agencies must designate a privacy contact"
- The privacy contact is *not* required to work full-time on privacy
- Designating contacts helps get the right information to the right people

Section 4 – Data discovery and documentation

Highlights

- "Agencies must understand the personal information they process"
- Existing requirements for data classification and inventorying support data discovery

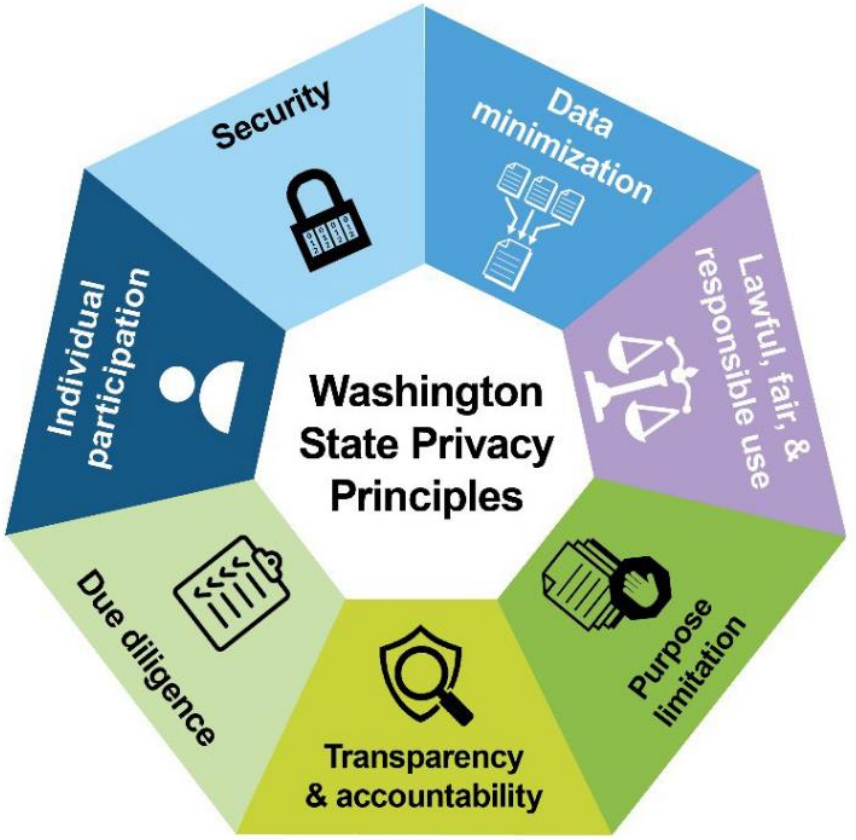
Resources

Managing personal information and reducing risk with data classification (webinar)

Section 5 – Policies and procedures

Highlights

- "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."
- Policies must ensure that privacy is integrated into activities and projects with personal information



Resources

- Washington State Agency Privacy Principles
- Washington State Agency Privacy Principles and Risk Management (webinar)
- Incorporating Privacy into the System Development Process (webinar)

Section 6 – Privacy assessments

Highlights

- Agencies must take steps to identify and address privacy risks
- Privacy threshold analysis (PTA) must be completed during any security design review that involves personal information
- Privacy impact assessment (PIA) required when PTA indicates potential for significant privacy risks

Resources

Privacy Threshold Analysis template

Privacy Threshold Analysis – Integrating privacy into security review (webinar)

Privacy Impact Assessments (webinar)

Section 7 – Training and awareness

Highlights

- Employees must receive basic privacy awareness training within 30 days of start date and at least annually
- Training requirement can be satisfied using OPDP training web-based training
- Additional training may be required based on role

Resources

Privacy Basics Training for Washington State Employees (video version)

Section 8 – Data sharing agreements

Highlights

- "Agencies must enter into written data sharing agreements when sharing category 3 or category 4 data outside the agency"
- Reflects existing law and existing state data sharing policy
- Send notice prior to OPDP prior to data sales

Resources

Washington State Data Sharing Policy

Data Sharing Agreement Implementation Guidance and Sample DSAs

Privacy and Data Sharing Agreement Best Practices Report (webinar)

Section 9 – Data disposal

Highlights

- "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."
- Incorporates existing requirement under Executive Order 16-01

Section 10 – Privacy notices

Highlights

- "Agencies must be transparent about how they process personal information by publishing privacy notices"
- Notices should provide meaningful, understandable information
- Routinely review and update as necessary to match current practices

Resources

Privacy Notices (webinar)

Section 11 – Individual participation

Highlights

- Agencies must allow people to access or control their information "to the extent consistent with applicable law and the government functions the agency performs"
- At a minimum agencies need procedures to receive and respond to requests to access or correct information

Section 12 – Incident response

Highlights

- Agencies must "implement adequate controls, including policies and training, to identify, report and respond to privacy incidents
- "Privacy incident" is broader than security incident, and includes any unauthorized use or disclosure even if doesn't impact an IT system

Resources

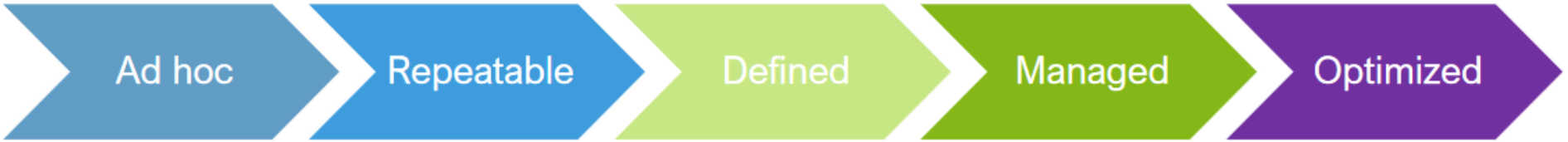
Washington's Data Breach Notification Law for State and Local Government (webinar)

State and Local Government Breach Assessment Form (template)

Section 13 – Monitoring and periodic review

Highlights

- "Agencies . . . must monitor and review privacy and data handling practices"
- Monitoring examples include metrics and auditing
- Review includes reviewing changes in processing activities, changes in technology, and changes in requirements



Resources

Frameworks for privacy success (webinar)

Measuring privacy (webinar)

Section 14 – Biometrics

Highlights

- Agencies must follow all applicable requirements for biometric identifiers
- Significant new requirements for agency use of facial recognition in 2020

Resources

Facial recognition – the good, the bad, and the regulated (webinar)

Chapter 43.386 RCW

WaTech
Washington Technology Solutions

Questions?

privacy@watech.wa.gov

www.watech.wa.gov/privacy