WaTech
Washington Technology Solutions

Privacy and Data Protection Background

New, Update or Sunset Review? 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 content was primarily adopted from industry standard privacy frameworks. The NIST Privacy Framework is a collaborative tool intended to help organizations identify and manage privacy risk. In 2022 the Office of Privacy and Data Protection adopted the Washington Privacy Framework, which is a simplified version of the NIST Privacy Framework. It is intended to help state agencies implement effective privacy practices. The content of this policy incorporates the foundational components of the Washington Privacy Framework that are appropriate for all state agencies.

The Office of Privacy and Data Protection also considered the data collected as part of its annual privacy assessment of state agencies and consulted with the Privacy Community of Practice and State Agency Privacy Forum.

What is the business case for the policy/standard?

Although there has been significant improvement in recent years, there is still a wide range of privacy maturity across the state agency enterprise. The benefits vary depending on each agency's current maturity:

- For agencies with strong, established privacy programs the new policy will more formally create baseline components to review and iterate on.
- For agencies with relatively new or incomplete privacy programs, the policy will help identify gaps and prioritize efforts.
- For agencies with few privacy practices in place, the policy will help identify and implement foundational privacy practices.

Agencies at all levels of the maturity scale have indicated that having privacy requirements in policy would help create internal momentum for prioritizing and communicate requirements to vendors.

What are the key objectives of the policy/standard?

The policy covers a range of foundational privacy practices. Key elements include:

- Designated privacy contacts
- Policies and procedures
- Privacy threshold analyses / privacy impact assessments (PTAs/PIAs)
- Training
- Data disposal
- Privacy notices
- Individual participation
- Incident response
- Monitoring
- Biometrics

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

Each state agency implementing baseline privacy protections is essential to the digital trust pillar of the Enterprise IT Strategic Plan. The digital trust pillar upholds and is interwoven in all of the 2023-2025 Enterprise IT Strategic plan goals.

What are the implementation considerations?

As measured by the Office of Privacy and Data Protection's annual privacy assessment of state agencies, most components of this policy are in place at most agencies. Most components already exist in statute, executive order, or state policy. Some agencies will need to take additional steps to comply with new requirements. The Office of Privacy and Data Protection has existing resources to help with implementation.

How will we know if the policy is successful?

The state will know if this policy is successful if agencies make progress on the policy requirements. This will be measured by data collected in the state's Annual Privacy Assessment Survey which asks about the specific policy requirements. Data collected from the most recent privacy assessment surveys already indicate that the privacy policy requirements are achievable. The policy requirements are both relevant and equitable given Washington's focus on digital equity and agencies collection and use of personal data. The year-over-year data from the annual privacy assessment and policy sunset review date will be used as the timeline for measuring policy success.