

# Frameworks for Privacy Success

---

Office of Privacy and Data Protection  
October 20, 2022

- **Privacy Framework and maturity model landscape**
- **Washington Privacy Framework goals**
- **Introduction to Washington Privacy Framework**
- **Privacy Framework uses and implementation**
- **Building a privacy program**

O  
P  
D  
P

# Privacy Framework and maturity model landscape

O  
P  
D  
P

# Frameworks – Foundations, Standards & Compliance

## Foundational Frameworks

- Fair Information Practice Principles (US Privacy Act)

## Standards

- NIST 800-53 (MARS-E, IRS Pub 1075, ACA)

## Compliance Schemas

- AICPA Privacy Maturity Framework (f/k/a Generally Accepted Privacy Principles)
- SOC II Type II Privacy Trust Service Criteria
- ISO 27701



# Frameworks - Taxonomy & Risk Management

## Taxonomy

- Solove's Taxonomy of Privacy

## Risk Management

- NIST Privacy Framework
- NISTIR 8063

O  
P  
D  
P

# Frameworks - Sectoral

## HIPAA

- Health information generated by Covered Entities

## FERPA

- Student education records

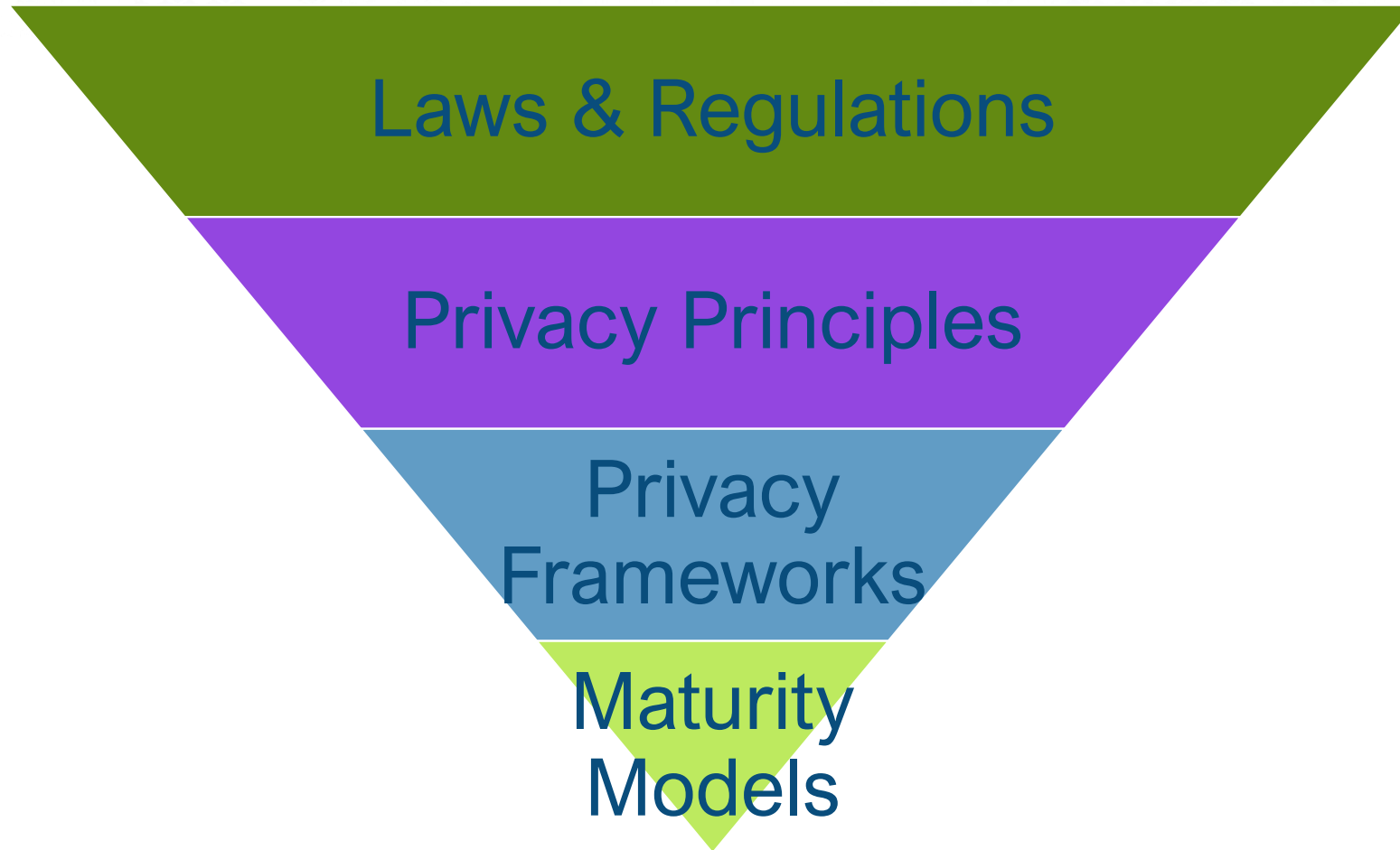
## COPPA

- Personal information on websites/online services for children under 13 years of age

O  
P  
D  
P

# Washington Privacy Framework goals

O  
P  
D  
P



# Effective Privacy and Data Protection

O  
P  
D  
P



# Why a Washington Privacy Framework

- **Reflect industry standards**
- **Approachable**
- **Scalable**
- **Flexible**



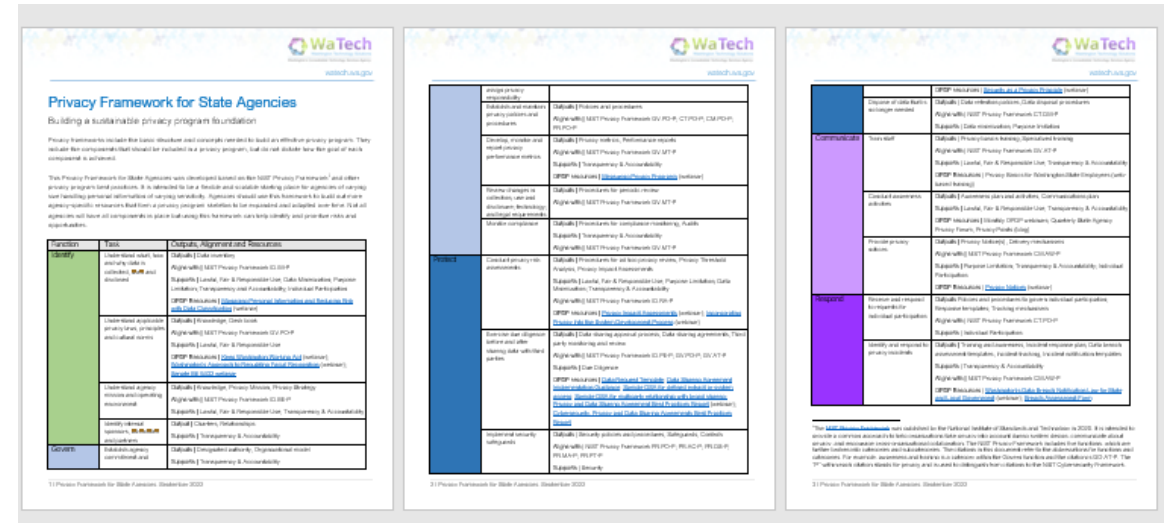
O  
P  
D  
P

# Introduction to Washington Privacy Framework

O  
P  
D  
P

# Privacy Framework for State Agencies

- Based on NIST Privacy Framework
- Provides high level direction (3 pages)
- Privacy Program Functions:
  - Identify
  - Govern
  - Protect
  - Communicate
  - Respond



The document is titled "Privacy Framework for State Agencies" and "Building a sustainable privacy program foundation". It includes an introduction and a table of functions and controls. The table is organized into five main functional areas: Identify, Govern, Protect, Communicate, and Respond. Each area has a list of specific functions and associated controls, with references to the NIST Privacy Framework (NIST SP 800-53) and the WaTech Privacy Framework (WTF).

Function	Tasks	Outputs, Alignment and Resources
Identify	Understand what has already been collected, stored and processed	<ul style="list-style-type: none"> <li>Default: Data Inventory</li> <li>Align with NIST Privacy Framework CS-DEP</li> <li>Supports: Locate, Fair &amp; Transparent Use, Data Minimization, Purpose Limitation, Transparency &amp; Accountability, Individual Participation</li> <li>WTF: <a href="#">WTF-010: Data Inventory</a> (Control)</li> </ul>
	Understand applicable privacy laws, principles and related norms	<ul style="list-style-type: none"> <li>Default: Knowledge, Governance</li> <li>Align with NIST Privacy Framework CI-FCP</li> <li>Supports: Locate, Fair &amp; Transparent Use</li> <li>WTF: <a href="#">WTF-011: Privacy Law &amp; Principle</a> (Control)</li> <li>WTF: <a href="#">WTF-012: Privacy Law &amp; Principle</a> (Control)</li> </ul>
	Understand agency mission and operating environment	<ul style="list-style-type: none"> <li>Default: Knowledge, Privacy Mission, Privacy Strategy</li> <li>Align with NIST Privacy Framework CS-DEP</li> <li>Supports: Locate, Fair &amp; Transparent Use, Transparency &amp; Accountability</li> <li>WTF: <a href="#">WTF-013: Privacy Mission</a> (Control)</li> </ul>
	Identify related systems, <b>WTF-014</b> and <b>WTF-015</b>	<ul style="list-style-type: none"> <li>Supports: Transparency &amp; Accountability</li> </ul>
Respond	Establish agency incident and	<ul style="list-style-type: none"> <li>Default: Computer Incident, Cyber Incident</li> <li>Supports: Transparency &amp; Accountability</li> </ul>

# Washington Privacy Framework Functions



O  
P  
D  
P

Function	Task	Outputs, Alignment and Resources
Identify	Understand what, how and why data is collected, used and disclosed	<p><b>Outputs</b>   Data inventory</p> <p><b>Aligns with</b>   NIST Privacy Framework ID.IM-P</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use; Data Minimization; Purpose Limitation; Transparency and Accountability; Individual Participation</p> <p><b>OPDP Resources</b>   <a href="#">Managing Personal Information and Reducing Risk with Data Classification</a> (webinar)</p>
	Understand applicable privacy laws, principles and cultural norms	<p><b>Outputs</b>   Knowledge; Deskbook</p> <p><b>Aligns with</b>   NIST Privacy Framework GV.PO-P</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use</p> <p><b>OPDP Resources</b>   <a href="#">Keep Washington Working Act</a> (webinar); <a href="#">Washington's Approach to Regulating Facial Recognition</a> (webinar); <a href="#">Senate Bill 5432 webinar</a></p>
	Understand agency mission and operating environment	<p><b>Outputs</b>   Knowledge, Privacy Mission, Privacy Strategy</p> <p><b>Aligns with</b>   NIST Privacy Framework ID.BE-P</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use; Transparency &amp; Accountability</p>
	Identify internal sponsors, advocates and partners	<p><b>Output</b>   Charters, Relationships</p> <p><b>Supports</b>   Transparency &amp; Accountability</p>

Function	Task	Outputs, Alignment and Resources
Identify	Understand what, how and why data is collected, used and disclosed	<p><b>Outputs</b>   Data inventory</p> <p><b>Aligns with</b>   NIST Privacy Framework ID.IM-P</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use; Data Minimization; Purpose Limitation; Transparency and Accountability; Individual Participation</p> <p><b>OPDP Resources</b>   <a href="#">Managing Personal Information and Reducing Risk with Data Classification</a> (webinar)</p>



Function	Task	Outputs, Alignment and Resources
Identify	Understand applicable privacy laws, principles and cultural norms	<p><b>Outputs</b>   Knowledge; Desk book</p> <p><b>Aligns with</b>   NIST Privacy Framework GV.PO-P</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use</p> <p><b>OPDP Resources</b>   <a href="#">Keep Washington Working Act</a> (webinar); <a href="#">Washington's Approach to Regulating Facial Recognition</a> (webinar); <a href="#">Senate Bill 5432</a> <a href="#">webinar</a></p>



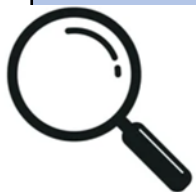
Function	Task	Outputs, Alignment and Resources
Identify	Understand agency mission and operating environment	<p><b>Outputs</b>   Knowledge, Privacy Mission, Privacy Strategy</p> <p><b>Aligns with</b>   NIST Privacy Framework ID.BE-P</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use; Transparency &amp; Accountability</p>
	Identify internal sponsors, advocates and partners	<p><b>Output</b>   Charters, Relationships</p> <p><b>Supports</b>   Transparency &amp; Accountability</p>





Function	Task	Outputs, Alignment and Resources
<b>Govern</b>	Establish agency commitment and assign privacy responsibility	<b>Outputs</b>   Designated authority, Organizational model <b>Supports</b>   Transparency & Accountability
	Establish and maintain privacy policies and procedures	<b>Outputs</b>   Policies and procedures <b>Aligns with</b>   NIST Privacy Framework GV.PO-P; CT.PO-P; CM.PO-P; PR.PO-P
	Develop, monitor and report privacy performance metrics	<b>Outputs</b>   Privacy metrics, Performance reports <b>Aligns with</b>   NIST Privacy Framework GV.MT-P <b>Supports</b>   Transparency & Accountability <b>OPDP resources</b>   <a href="#">Measuring Privacy Programs</a> (webinar)
	Review changes in collection, use and disclosure; technology; and legal requirements	<b>Outputs</b>   Procedures for periodic review <b>Aligns with</b>   NIST Privacy Framework GV.MT-P
	Monitor compliance	<b>Outputs</b>   Procedures for compliance monitoring, Audits <b>Supports</b>   Transparency & Accountability <b>Aligns with</b>   NIST Privacy Framework GV.MT-P

Function	Task	Outputs, Alignment and Resources
<b>Govern</b>	Establish agency commitment and assign privacy responsibility	<p><b>Outputs</b>   Designated authority, Organizational model</p> <p><b>Supports</b>   Transparency &amp; Accountability</p>
	Establish and maintain privacy policies and procedures	<p><b>Outputs</b>   Policies and procedures</p> <p><b>Aligns with</b>   NIST Privacy Framework GV.PO-P; CT.PO-P; CM.PO-P; PR.PO-P</p>



Function	Task	Outputs, Alignment and Resources
<b>Govern</b>	Develop, monitor and report privacy performance metrics	<p><b>Outputs</b>   Privacy metrics, Performance reports</p> <p><b>Aligns with</b>   NIST Privacy Framework GV.MT-P</p> <p><b>Supports</b>   Transparency &amp; Accountability</p> <p><b>OPDP resources</b>   <a href="#">Measuring Privacy Programs</a> (webinar)</p>



Function	Task	Outputs, Alignment and Resources
<b>Govern</b>	Review changes in collection, use and disclosure; technology; and legal requirements	<p><b>Outputs</b>   Procedures for periodic review</p> <p><b>Aligns with</b>   NIST Privacy Framework GV.MT-P</p>
	Monitor compliance	<p><b>Outputs</b>   Procedures for compliance monitoring, Audits</p> <p><b>Supports</b>   Transparency &amp; Accountability</p> <p><b>Aligns with</b>   NIST Privacy Framework GV.MT-P</p>



Function	Task	Outputs, Alignment and Resources
Protect	Conduct privacy risk assessments	<p><b>Outputs</b>   Procedures for ad hoc privacy review, Privacy Threshold Analysis, Privacy Impact Assessments</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use; Purpose Limitation; Data Minimization; Transparency &amp; Accountability</p> <p><b>Aligns with</b>   NIST Privacy Framework ID.RA-P</p> <p><b>OPDP resources</b>   <a href="#">Privacy Impact Assessments</a> (webinar); <a href="#">Incorporating Privacy Into the System Development Process</a> (webinar)</p>
	Exercise due diligence before and after sharing data with third parties	<p><b>Outputs</b>   Data sharing approval process, Data sharing agreements, Third party monitoring and review</p> <p><b>Aligns with</b>   NIST Privacy Framework ID.PE-P; GV.PO-P; GV.AT-P</p> <p><b>Supports</b>   Due Diligence</p> <p><b>OPDP resources</b>   <a href="#">Data Request Template</a>; <a href="#">Data Sharing Agreement Implementation Guidance</a>; <a href="#">Sample DSA for defined extract or system access</a>; <a href="#">Sample DSA for multiparty relationship with broad sharing</a>; <a href="#">Privacy and Data Sharing Agreement Best Practices Report</a> (webinar); <a href="#">Cybersecurity, Privacy and Data Sharing Agreements Best Practices Report</a></p>

Function	Task	Outputs, Alignment and Resources
Protect	Implement security safeguards	<p><b>Outputs</b>   Security policies and procedures, Safeguards, Controls</p> <p><b>Aligns with</b>   NIST Privacy Framework PR.PO-P; PR.AC-P; PR.DS-P; PR.MA-P; PR.PT-P</p> <p><b>Supports</b>   Security</p> <p><b>OPDP resources</b>   <a href="#">Security as a Privacy Principle</a> (webinar)</p>
	Dispose of data that is no longer needed	<p><b>Outputs</b>   Data retention policies, Data disposal procedures</p> <p><b>Aligns with</b>   NIST Privacy Framework CT.DM-P</p> <p><b>Supports</b>   Data minimization; Purpose limitation</p>

Function	Task	Outputs, Alignment and Resources
Protect	Conduct privacy risk assessments	<p><b>Outputs</b>   Procedures for ad hoc privacy review, Privacy Threshold Analysis, Privacy Impact Assessments</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use; Purpose Limitation; Data Minimization; Transparency &amp; Accountability</p> <p><b>Aligns with</b>   NIST Privacy Framework ID.RA-P</p> <p><b>OPDP resources</b>   <a href="#">Privacy Impact Assessments</a> (webinar); <a href="#">Incorporating Privacy Into the System Development Process</a> (webinar)</p>



Function	Task	Outputs, Alignment and Resources
Protect	Exercise due diligence before and after sharing data with third parties	<p><b>Outputs</b>   Data sharing approval process, Data sharing agreements, Third party monitoring and review</p> <p><b>Aligns with</b>   NIST Privacy Framework ID.PE-P; GV.PO-P; GV.AT-P</p> <p><b>Supports</b>   Due Diligence</p> <p><b>OPDP resources</b>   <a href="#">Data Request Template</a>; <a href="#">Data Sharing Agreement Implementation Guidance</a>; <a href="#">Sample DSA for defined extract or system access</a>; <a href="#">Sample DSA for multiparty relationship with broad sharing</a>; <a href="#">Privacy and Data Sharing Agreement Best Practices Report</a> (webinar); <a href="#">Cybersecurity, Privacy and Data Sharing Agreements Best Practices Report</a></p>





Function	Task	Outputs, Alignment and Resources
Protect	Implement security safeguards	<p><b>Outputs</b>   Security policies and procedures, Safeguards, Controls</p> <p><b>Aligns with</b>   NIST Privacy Framework PR.PO-P; PR.AC-P; PR.DS-P; PR.MA-P; PR.PT-P</p> <p><b>Supports</b>   Security</p> <p><b>OPDP resources</b>   <a href="#">Security as a Privacy Principle</a> (webinar)</p>



Function	Task	Outputs, Alignment and Resources
<b>Protect</b>	Dispose of data that is no longer needed	<p><b>Outputs</b>   Data retention policies, Data disposal procedures</p> <p><b>Aligns with</b>   NIST Privacy Framework CT.DM-P</p> <p><b>Supports</b>   Data minimization; Purpose limitation</p>



Function	Task	Outputs, Alignment and Resources
Communicate	Train staff	<p><b>Outputs</b>   Privacy basics training, Specialized training</p> <p><b>Aligns with</b>   NIST Privacy Framework GV.AT-P</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use; Transparency &amp; Accountability</p> <p><b>OPDP Resources</b>   Privacy Basics for Washington State Employees (web-based training)</p>
	Conduct awareness activities	<p><b>Outputs</b>   Awareness plan and activities, Communications plan</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use; Transparency &amp; Accountability</p> <p><b>OPDP resources</b>   Monthly OPDP webinars; Quarterly State Agency Privacy Forum, Privacy Points (blog)</p>
	Provide privacy notices	<p><b>Outputs</b>   Privacy Notice(s), Delivery mechanisms</p> <p><b>Aligns with</b>   NIST Privacy Framework CM.AW-P</p> <p><b>Supports</b>   Purpose Limitation; Transparency &amp; Accountability; Individual Participation</p> <p><b>OPDP Resources</b>   <a href="#">Privacy Notices</a> (webinar)</p>

Function	Task	Outputs, Alignment and Resources
Communi- cate	Train staff	<p><b>Outputs</b>   Privacy basics training, Specialized training</p> <p><b>Aligns with</b>   NIST Privacy Framework GV.AT-P</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use; Transparency &amp; Accountability</p> <p><b>OPDP Resources</b>   Privacy Basics for Washington State Employees (web-based training)</p>



Function	Task	Outputs, Alignment and Resources
Communi- cate	Conduct awareness activities	<p><b>Outputs</b>   Awareness plan and activities, Communications plan</p> <p><b>Supports</b>   Lawful, Fair &amp; Responsible Use; Transparency &amp; Accountability</p> <p><b>OPDP resources</b>   Monthly OPDP webinars; Quarterly State Agency Privacy Forum, Privacy Points (blog)</p>



Function	Task	Outputs, Alignment and Resources
<p>Communi- cate</p>	<p>Provide privacy notices</p>	<p><b>Outputs</b>   Privacy Notice(s), Delivery mechanisms</p> <p><b>Aligns with</b>   NIST Privacy Framework CM.AW-P</p> <p><b>Supports</b>   Purpose Limitation; Transparency &amp; Accountability; Individual Participation</p> <p><b>OPDP Resources</b>   <a href="#">Privacy Notices</a> (webinar)</p>




Function	Task	Outputs, Alignment and Resources
Respond	Receive and respond to requests for individual participation	<p><b>Outputs</b> Policies and procedures to govern individual participation; Response templates; Tracking mechanisms</p> <p><b>Aligns with</b>   NIST Privacy Framework CT.PO-P</p> <p><b>Supports</b>   Individual Participation</p>
	Identify and respond to privacy incidents	<p><b>Outputs</b>   Training and awareness, Incident response plan, Data breach assessment templates, Incident tracking, Incident notification templates</p> <p><b>Supports</b>   Transparency &amp; Accountability</p> <p><b>Aligns with</b>   NIST Privacy Framework CM.AW-P</p> <p><b>OPDP Resources</b>   <a href="#">Washington's Data Breach Notification Law for State and Local Government</a> (webinar); <a href="#">Breach Assessment Form</a></p>

Function	Task	Outputs, Alignment and Resources
<b>Respond</b>	Receive and respond to requests for individual participation	<p><b>Outputs</b> Policies and procedures to govern individual participation; Response templates; Tracking mechanisms</p> <p><b>Aligns with</b>   NIST Privacy Framework CT.PO-P</p> <p><b>Supports</b>   Individual Participation</p>





Function	Task	Outputs, Alignment and Resources
<b>Respond</b> 	Identify and respond to privacy incidents	<p><b>Outputs</b>   Training and awareness, Incident response plan, Data breach assessment templates, Incident tracking, Incident notification templates</p> <p><b>Supports</b>   Transparency &amp; Accountability</p> <p><b>Aligns with</b>   NIST Privacy Framework CM.AW-P</p> <p><b>OPDP Resources</b>   <a href="#">Washington's Data Breach Notification Law for State and Local Government</a> (webinar); <a href="#">Breach Assessment Form</a></p>

# Privacy Framework Uses and Implementation

O  
P  
D  
P

# Options and benefits

- Gap analysis
- Identify risks and opportunities
- Document existing activities and set targets for improvements
- Consistent communication mechanism
- Review supplemental guidance

O  
P  
D  
P

## Identify – Understand what, how and why data is collected, used and disclosed

Outputs, Alignment and Resources

**Outputs** | Data inventory

**Aligns with** | NIST Privacy Framework ID.IM-P

**Supports** | Lawful, Fair & Responsible Use; Data Minimization; Purpose Limitation; Transparency and Accountability; Individual Participation

**OPDP Resources** | [Managing Personal Information and Reducing Risk with Data Classification](#) (webinar)

Supplemental Guidance

Understanding the types of information collected, how it is collected, its location and the purposes it is used for is essential for effective privacy risk management. It enables improved efforts to minimize data, limit uses to the original reason it was collected, ensure appropriate use, respond to individuals who request access to their own information, and respond to incidents.

Systems that process data should be inventoried. Data inventories should include the types of information included, the purposes for collecting and using the data, data sources, data classification, the categories of individuals whose information is processed and data owners.

This information should be documented when new systems are developed, or when there are changes to existing systems or the way they are used. Inventories should be routinely updated. Possible sources for compiling data inventories include existing application inventories, questionnaires or interviews, automated tools and collection processes such as privacy impact assessments.

## **Govern** – Establish agency commitment and assign privacy responsibility

Outputs, Alignment and Resources

**Outputs** | Designated authority, Organizational model

**Supports** | Transparency & Accountability

Supplemental Guidance

Agency leadership can demonstrate a commitment to privacy by providing appropriate resources to ensure privacy is not an additional duty assigned to individuals without the skills or time to perform privacy functions.

The appropriate privacy staffing model varies significantly from agency to agency, based primarily on agency size, overall organizational structure, the types of personal information maintained, and applicable legal requirements for that personal information.

Agencies should assign privacy duties in a manner that is consistent with overall agency structure. For example, an agency with strong central governance of activities like contracting and information technology should first consider a centralized model, while an agency with divisions or administrations that operate largely independently may prefer a central privacy office with embedded staff performing privacy functions across the agency.

Regardless of the model chosen, a designated privacy point of contact can serve as a liaison with the state Office of Privacy and Data Protection, helps prevent gaps in privacy practices and ensures accountability.

## Communicate – Conduct awareness activities

Outputs, Alignment and Resources

**Outputs** | Awareness plan and activities, Communications plan

**Supports** | Lawful, Fair & Responsible Use; Transparency & Accountability

**OPDP resources** | Monthly OPDP webinars; Quarterly State Agency Privacy Forum, Privacy Points (blog)

Supplemental Guidance

Awareness activities are routinely planned to keep privacy and data protection top of mind for agency staff. Awareness activities are less formal than training activities, and may include things like signs, informal meetings or intranet or email updates.

Agency communication channels should be understood and utilized to target activities to different groups, such as all staff or agency leaders. Materials developed by the Office of Privacy and Data Protection, such as activities related to Data Privacy Day each January can be distributed to leverage limited resources.

# Building a Privacy Program

O  
P  
D  
P

# Washington Privacy Framework Functions



O  
P  
D  
P



# Privacy Program Development

Identify roles within your organization that are central to data management or data governance. This is part of “Govern” function:

- Legal
- Risk
- IT
- Security
- Records (retention, management, public)
- Data or information governance
- Compliance
- Others?

O  
P  
D  
P

# Ask?

## Does your agency have an identified privacy officer?

- Yes
- No
- Partial

## Does your agency have an incident response plan?

- Yes
- No
- Under development

O  
P  
D  
P

# Privacy is Interdisciplinary

- Look at your [data] incident response plan
- Current data handling policies
  - Who would you report a data incident to?
  - Within how much time? A day? A week?
- Training on data handling and confidentiality
- Nondisclosure Agreements
- Privacy Principles

O  
P  
D  
P

# Program Development

- Look at the positions you already have
- Look at the policies you already have
- Identify what information you need to protect
- Build a community within those resources
  - Regular meetings
  - Regular trainings
  - Build the culture
  - Build the expertise
- Security
- Incident Response
- Use Foundational Principles



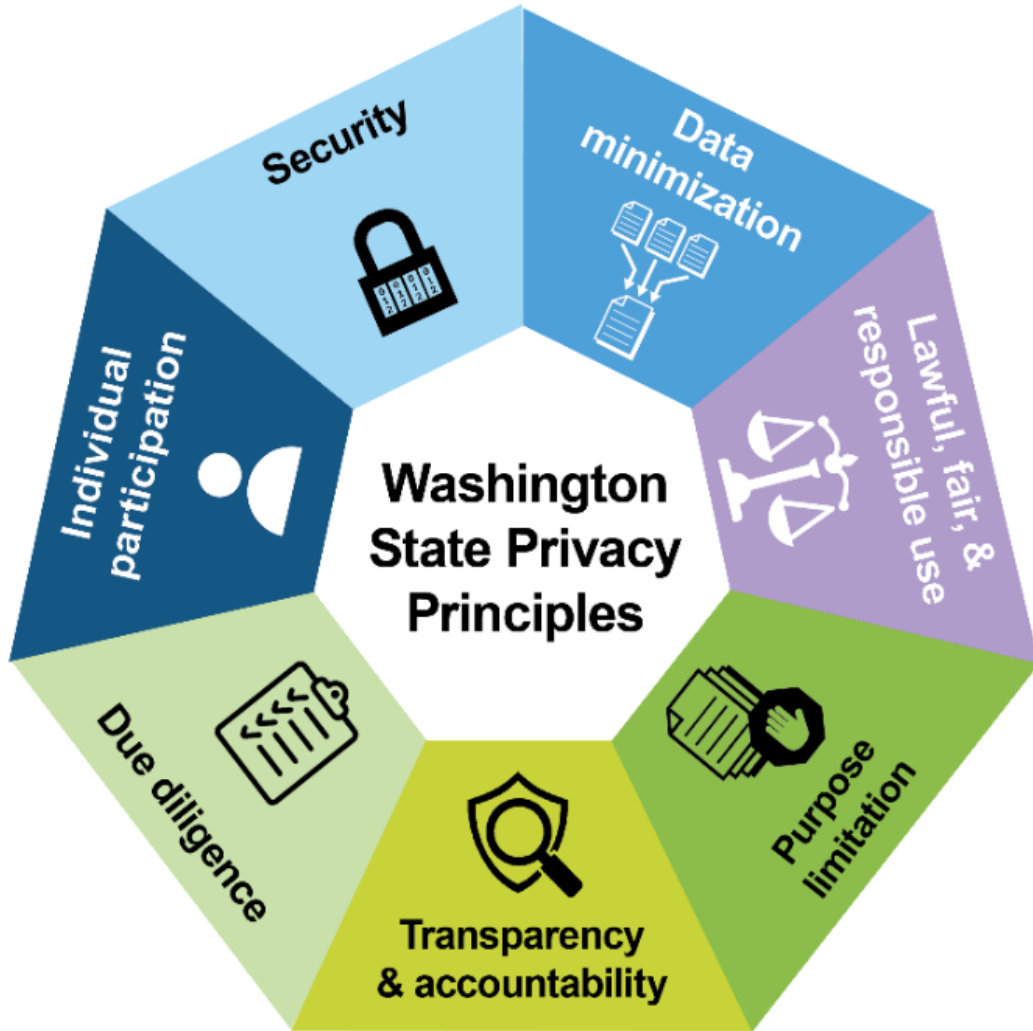
O  
P  
D  
P

# Program Development

- Look at the positions you already have **[Govern]**
- Look at the policies you already have **[Govern]**
- Identify what information you need to protect **[Identify]**
- Build a community within those resources **[Communicate]**
  - Regular meetings
  - Regular trainings
  - Build the culture
  - Build the expertise
- Security **[Protect]**
- Incident Response **[Respond]**
- Use Foundational Principles **[Identify]**



O  
P  
D  
P



- **Use Washington State Agency Privacy Principles as well for your starting place.**
- **Align current agency mission and identify applicable laws and data sets need most protection.**

[Washington Privacy Principles](#)

O  
P  
D  
P

Thank you

Questions?

O  
P  
D  
P