Privacy Framework for State Agencies

Building a sustainable privacy program foundation

Privacy frameworks include the basic structure and concepts needed to build an effective privacy program. They include the components that should be included in a privacy program, but do not dictate how the goal of each component is achieved.

This Privacy Framework for State Agencies was developed based on the NIST Privacy Framework[i] and other privacy program best practices. It is intended to be a flexible and scalable starting place for agencies of varying size handling personal information of varying sensitivity. Agencies should use this framework to build out more agency-specific resources that form a privacy program skeleton to be expanded and adapted over time. Not all agencies will have all components in place but using this framework can help identify and prioritize risks and opportunities.

Function	Task	Outputs, Alignment and Resources
Identify	Understand what, how and why data is collected, used and disclosed	**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)
	Understand applicable privacy laws, principles and cultural norms	**Outputs** | Knowledge; Desk book **Aligns with** | NIST Privacy Framework GV.PO-P **Supports** | Lawful, Fair & Responsible Use **OPDP Resources** | Keep Washington Working Act (webinar); Washington's Approach to Regulating Facial Recognition (webinar); Senate Bill 5432 webinar
	Understand agency mission and operating environment	**Outputs** | Knowledge, Privacy Mission, Privacy Strategy **Aligns with** | NIST Privacy Framework ID.BE-P **Supports** | Lawful, Fair & Responsible Use; Transparency & Accountability
	Identify internal sponsors, advocates and partners	**Output** | Charters, Relationships **Supports** | Transparency & Accountability
Govern	Establish agency commitment and assign privacy responsibility	**Outputs** | Designated authority, Organizational model **Supports** | Transparency & Accountability

Govern	Establish and maintain privacy policies and procedures	**Outputs** | Policies and procedures **Aligns with** | NIST Privacy Framework GV.PO-P; CT.PO-P; CM.PO-P; PR.PO-P
	Develop, monitor and report privacy performance metrics	**Outputs** | Privacy metrics, Performance reports **Aligns with** | NIST Privacy Framework GV.MT-P **Supports** | Transparency & Accountability **OPDP resources** | Measuring Privacy Programs (webinar)
	Review changes in collection, use and disclosure; technology; and legal requirements	**Outputs** | Procedures for periodic review **Aligns with** | NIST Privacy Framework GV.MT-P
	Monitor compliance	**Outputs** | Procedures for compliance monitoring, Audits **Supports** | Transparency & Accountability **Aligns with** | NIST Privacy Framework GV.MT-P
Protect	Conduct privacy risk assessments	**Outputs** | Procedures for ad hoc privacy review, Privacy Threshold Analysis, Privacy Impact Assessments **Supports** | Lawful, Fair & Responsible Use; Purpose Limitation; Data Minimization; Transparency & Accountability **Aligns with** | NIST Privacy Framework ID.RA-P **OPDP resources** | Privacy Impact Assessments (webinar); Incorporating Privacy Into the System Development Process (webinar)
	Exercise due diligence before and after sharing data with third parties	**Outputs** | Data sharing approval process, Data sharing agreements, Third party monitoring and review **Aligns with** | NIST Privacy Framework ID.PE-P; GV.PO-P; GV.AT-P **Supports** | Due Diligence **OPDP resources** | Data Request Template; Data Sharing Agreement Implementation Guidance; Sample DSA for defined extract or system access; Sample DSA for multiparty relationship with broad sharing; Privacy and Data Sharing Agreement Best Practices Report (webinar); Cybersecurity, Privacy and Data Sharing Agreements Best Practices Report
	Implement security safeguards	**Outputs** | Security policies and procedures, Safeguards, Controls **Aligns with** | NIST Privacy Framework PR.PO-P; PR.AC-P; PR.DS-P; PR.MA-P; PR.PT-P **Supports** | Security **OPDP resources** | Security as a Privacy Principle (webinar)

Protect	Dispose of data that is no longer needed	**Outputs** | Data retention policies, Data disposal procedures **Aligns with** | NIST Privacy Framework CT.DM-P **Supports** | Data minimization; Purpose limitation
Communicate	Train staff	**Outputs** | Privacy basics training, Specialized training **Aligns with** | NIST Privacy Framework GV.AT-P **Supports** | Lawful, Fair & Responsible Use; Transparency & Accountability **OPDP Resources** | Privacy Basics for Washington State Employees (web-based training)
	Conduct awareness activities	**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)
	Provide privacy notices	**Outputs |** Privacy Notice(s), Delivery mechanisms **Aligns with |** NIST Privacy Framework CM.AW-P **Supports |** Purpose Limitation; Transparency & Accountability; Individual Participation **OPDP Resources** | Privacy Notices (webinar)
Respond	Receive and respond to requests for individual participation	**Outputs** Policies and procedures to govern individual participation; Response templates; Tracking mechanisms **Aligns with** | NIST Privacy Framework CT.PO-P **Supports** | Individual Participation
	Identify and respond to privacy incidents	**Outputs |** Training and awareness, Incident response plan, Data breach assessment templates, Incident tracking, Incident notification templates **Supports** | Transparency & Accountability **Aligns with |** NIST Privacy Framework CM.AW-P **OPDP Resources** | Washington's Data Breach Notification Law for State and Local Government (webinar); Breach Assessment Form

[i] The NIST Privacy Framework was published by the National Institute of Standards and Technology in 2020. It is intended to provide a common approach to help organizations take privacy into account during system design, communicate about privacy, and encourage cross-organizational collaboration. The NIST Privacy Framework includes five functions, which are further broken into categories and subcategories. The citations in this document refer to the abbreviations for functions and categories. For example, awareness and training is a category within the Govern function and the citation is GO.AT-P. The "P" within each citation stands for privacy and is used to distinguish from citations to the NIST Cybersecurity Framework.