WaTech
Washington Technology Solutions
*Washington's Consolidated Technology Services Agency*

# Privacy and Cybersecurity Best Practices

December 2021

# Table of contents

# Introduction

Chapter 291, Laws of 2021, established WaTech's state Office of Cybersecurity (OCS) as the state's lead organization in combatting cyber threats and created a clear mandate for the development of centralized services and functions across state government.

Section 4 requires OCS to research, examine and report on existing data protection best practices in collaboration with the Office of Privacy and Data Protection (OPDP) and the Office of the Attorney General. Specifically, the report must contemplate:

> …best practices for data governance, data protection, the sharing of data relating to cybersecurity, and the protection of state and local governments' information technology systems and infrastructure including, but not limited to, model terms for data-sharing contracts and adherence to privacy principles.

**ESSB 5432 Section 4 requires OCS and its partners to provide information on:**

- Best practices for data governance.
- Data protection.
- The sharing of data related to cybersecurity.
- The protection of state and local governments' information technology systems and infrastructure.

This report is divided into three sections:

- Cybersecurity: Section one discusses current cybersecurity threats and trends, key findings that identify areas for improvement, and recommendations based on leading industry best practices for closing gaps and improving the state's security posture.
- Privacy: Section two provides an overview of existing privacy principles and opportunities to further strengthen adherence, as well as background on existing privacy frameworks and maturity models.
- Data sharing: Section three addresses new and existing data sharing agreement requirements. It includes steps agencies can take to identify when a data sharing agreement is needed, and effectively implement and monitor agreements.

While this report includes best practices and guidance that agencies can use to improve cybersecurity and privacy activities, it does not carry the effect of law and is not legal advice.

# Section One: Cybersecurity

## Cybersecurity threats and trends

With more than 100 state agencies serving a population of nearly eight million people, the state of Washington has one of the largest and fastest growing service delivery systems in the nation. State agencies utilize a vast number of information technology and operational technology systems to provide services to Washingtonians and to protect their data.

The state has evolved from systems predominantly residing in the state data center utilizing the state governmental network (SGN) to a more distributed system environment utilizing the public cloud and vendor data center environments.

**State of Washington - technology footprint:**

- 200,000 operational technology systems (laptops, desktops, servers, network devices).
- 6,000 information technology systems, including:
  - 800 vendor software applications.
- 700 suppliers.

Washington state has a large and growing technology footprint. The enormous amount of data generated by the enterprise is stored not only on the SGN and within the confines of the state data center, but also in the public cloud and third-party vendors' data centers. . Our technology systems and the large amount of data must be protected throughout its lifecycle, and by every individual accessing the systems and corresponding data. Standardized enterprise data governance is critical to manage and safeguard the information entrusted to us by Washingtonians.

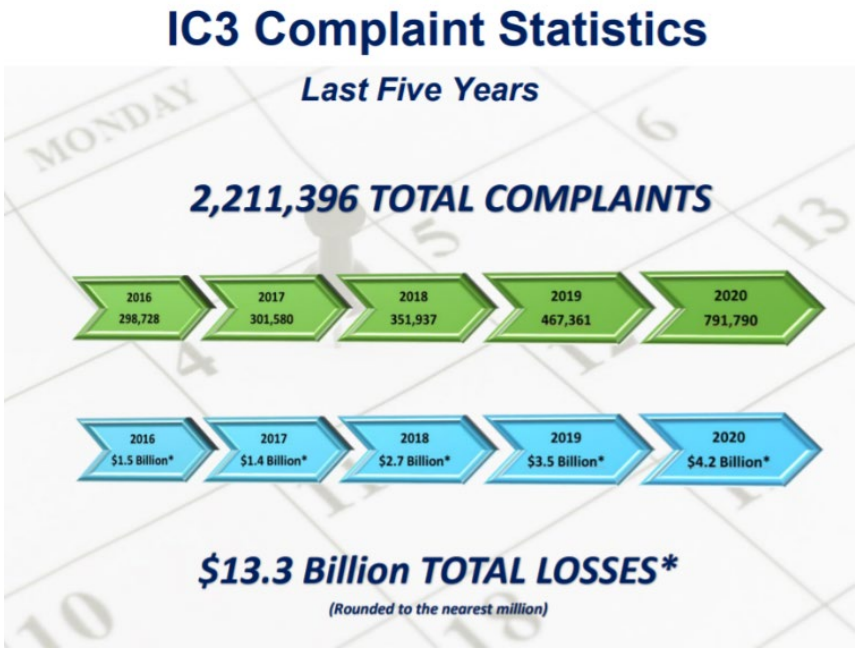
Washington faces persistent and increasingly sophisticated cyberattacks that threaten state agencies and private vendors that state agencies partner with – an ongoing threat that ultimately impacts the security and privacy of Washingtonians.

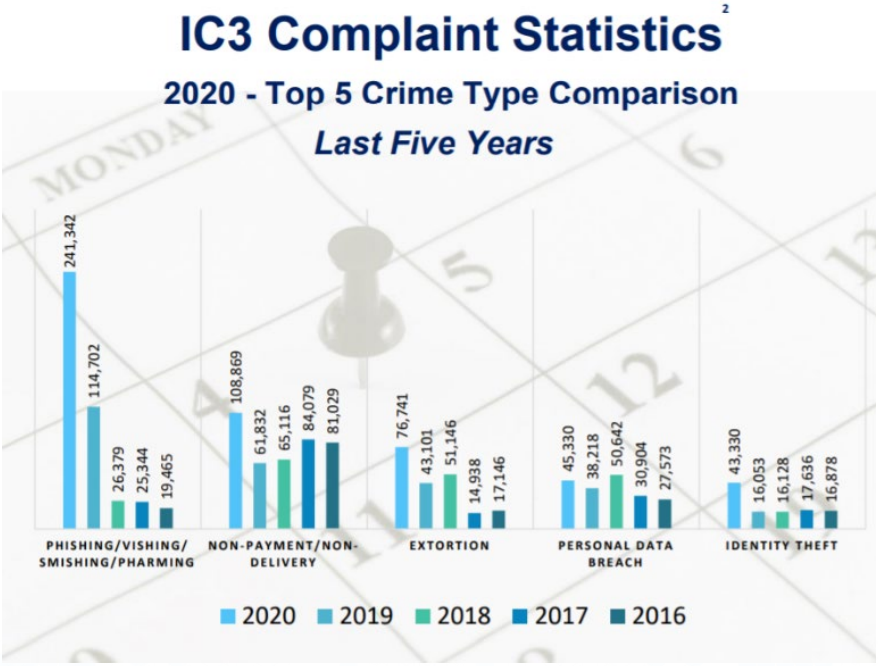
According to the Washington State Attorney General's Office 2021 Data Breach Report, the number of data breaches reported to the AG's office skyrocketed to 280 in 2021 compared to the previous year's total of 60. The report found that more than 150 ransomware incidents were recorded in 2021. Washington state law requires all public and private organizations impacted by a data breach to notify Washingtonians whose personal information was compromised, as well as the Attorney General's Office, if more than 500 people were impacted by the breach.

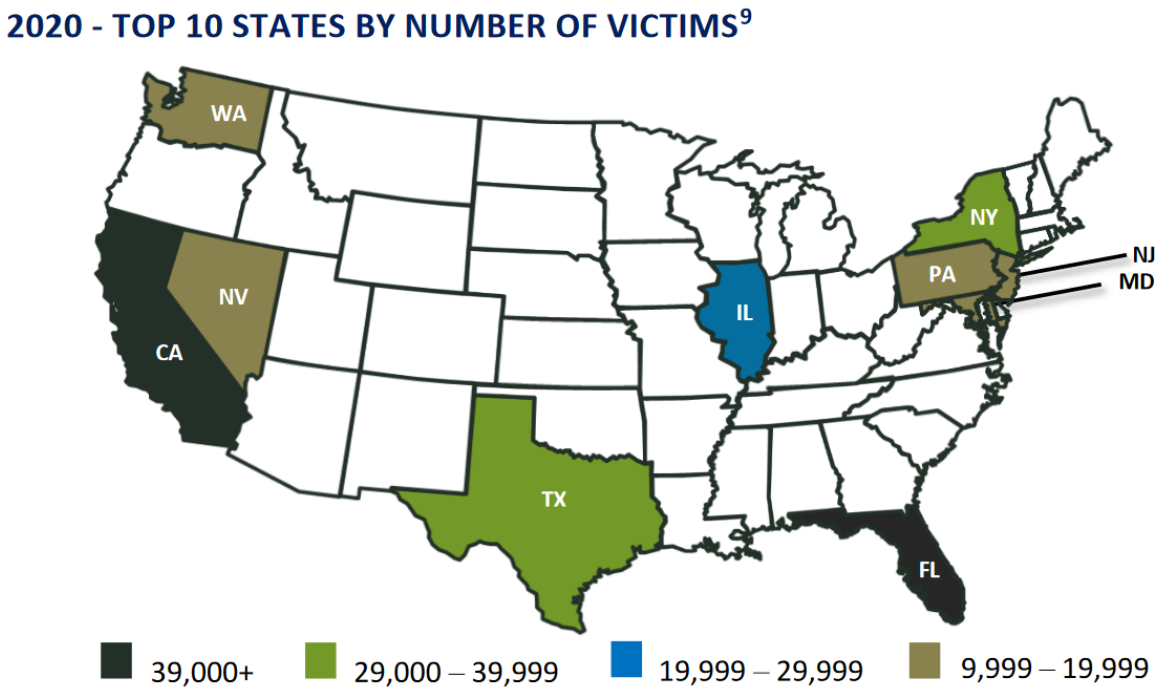
Nationally, according to the Federal Bureau of Investigations' 2020 Internet Crime Report, a record number of complaints were received from the American public in 2020 – 791,790 reported losses exceeding $4.1 billion. That represented a 69% increase in total complaints from 2019. Business Email Compromise (BEC) schemes continued to be the costliest with 19,369 complaints amounting to an adjusted loss of approximately $1.8 billion. Phishing scams were also prominent with 241,342 complaints, and ransomware incidents continued to rise with 2,474 incidents reported in 2020.

According to the 2020 Internet Crime Complaint Center (IC3) report – IC3 received over 28,500 complaints related to COVID-19 nationwide. Fraudsters targeted the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), which included provisions to help small businesses during the pandemic. The IC3 received thousands of complaints reporting emerging financial crime revolving around CARES Act stimulus funds, specifically targeting unemployment insurance, Paycheck Protection Program (PPP) loans, and Small

Business Economic Injury Disaster Loans, as well as other COVID-related fraud. The IC3 charts below show overall complaint statistics and complaints by crime.






*Top 10 states based on number of victims reporting the crime to FBI.*

The Verizon Data Breach Investigations Report (DBIR), one of industry's top reports, provides annual analysis of security incidents and breaches. This report has indicated for many years that public sector ranks high for the most security incidents and data breaches.

| Year | 2020 | 2021 |
|---|---|---|
| Security Incidents | 6,843 | 3,236 |
| Confirmed Data Breaches | 346 | 885 |

By far the biggest threat for any organization is social engineering. Threat actors have become increasingly sophisticated in crafting phishing emails that attempt to trick people into downloading malware or provide account credentials. Social engineering now accounts for 69% of breaches in the public sector, according to the 2021 DBIR.

The success of social engineering attacks is heavily driven by the implicit trust (the user is known and is inside the organization's security perimeter). Most social engineering attacks are successful because the phishing email is sent from a compromised email account. For people receiving email from a compromised account, it looks like the message came from a trusted source. In this digital age, everyone has multiple online accounts. Often, we find that people reuse the same credentials for multiple accounts. Bad actors take advantage of this by using data obtained in the data breach of one organization to compromise accounts in other organizations.

What is the primary goal of this malicious activity? Identity theft. It is the biggest threat impacting the security and privacy of people in our state. If bad actors can compromise and steal an identity, especially one with administrative privileges, the malicious actors can then enter and traverse the organization's network. Stolen identities are also the root cause for fraud. The massive data breaches that have occurred nationally have had a cascading effect. Personally Identifiable Information (PII) stolen by threat actors is readily available for purchase on the dark web, which is then utilized to launch new cyberattacks. In Washington state, criminals used this type of recycled PII to fraudulently file unemployment benefits in 2020. At the same time, technological changes have opened more avenues for bad actors to attack state systems. Accelerated by work-from-home initiatives, our workforce has modernized toward accessing the State Government Network (SGN) from home using the internet. Agencies have adopted remote business and engagement due to social distancing measures, putting higher risk transactions that would otherwise mandate in-person interactions into an exclusively remote context. Now, with nearly 800 information technology systems already in the cloud, our state's center of gravity for data and applications is steadily moving out of the state's data center and into the cloud.

This transformational change in how the state does business and provides services also requires a rapid and foundational shift in identity management. The proliferation of ransomware attacks across the nation in 2020 and 2021 shows that our adversaries are more motivated than ever. Bad actors are introducing increasingly damaging tactics, techniques, and procedures. They are adding more tools to their arsenals and forming alliances with other bad actor organizations to bolster their strength and extend reach. Studies show it only takes bad actors an average of 9.5 hours to breach a network. However, it takes 280 days for the organization attacked to identify and contain a breach because they lack the visibility and tools needed to rapidly detect and respond to a security incident.

Conclusion: In large part due to the COVD-19 pandemic, the way the state conducts business – and the way Washingtonians access services – has undergone unprecedented change. This, in turn, raises new risks that require the state to proactively take steps to protect its data and systems.

## Key Findings

1) Data Governance needs to be adaptive. The scale and speed of digital business demands has dramatically increased over the last couple of years and the pandemic accelerated those demands. Due to the state's federated model, data governance practices are localized and inconsistent across agencies. We lack a standard approach to assess, measure, monitor, and report the progress of data governance. Regulatory and compliance requirements are playing a major role for data governance at the agency level and in turn influencing enterprise level decisions.

**Key Findings:**

- The "implicit trust" model is no longer an option.
- Improve visibility to threats.
- Security needs to be managed in the context of risk to business.

2) Implicit trust is no longer an option. The implicit trust inherent in many of our information technology systems and infrastructure needs to be systematically removed and replaced with a zero-trust model. The implicit trust model does not provide the level of security controls that is necessary in today's organizational environment because it increases the risk of malware infections and the potential for an attack to spread. Although implicit trust may have been effective in a data center (on-premises environment), that is not true given today's hybrid workforce and the use of cloud services.

3) Improve visibility to threats. Due to the federated nature of our state government, with each agency largely responsible for maintaining and securing its own IT systems, the state is challenged in its ability to detect and respond to threats. It is critical for the state, at an enterprise level, to be able to monitor its entire ecosystem for rapid detection and response. The state needs that level of visibility, and a modernized tool set, to match the growing speed and sophistication of its adversaries. Washington State CIO Bill Kehoe said "My experience is that when you're federated around security services, each agency has its own culture and its own sense of urgency around security and how they apply controls. When an organization moves that to an enterprise service model, a standardized, consistent, and higher level of monitoring and urgency throughout the whole state is evident."

4) Security needs to be managed in the context of risk to business. Agencies need to move away from a compliance-based approach to a risk-based approach. A risk-based approach to managing security program encompasses the agency's business, its mission, it's needs and priorities in the overall context of security decisions. The business impact from security attacks is significantly different for each agency. As the state rapidly moves ahead with transforming state services through digital initiatives, which will include the use of vendors, agency leaders need access to methods to accurately quantify cybersecurity risks holistically as part of the decision-making process.

## Recommendations based on best practices

- Centralize and Standardize Data Governance: The state of Washington can benefit from a centralized form of data governance that would identify and prioritize desired business outcomes at both the agency and enterprise level. For example, if the state's intended business outcome is having an enhanced digital experience, we cannot just focus on decisions to improve the functionality of a system or asset in an agency. The state needs analytical data, such as data from security tool that is telling us why a system is attacked more often, or data from an operational tool that explains why a particular system goes offline more often than others. With that in mind, we need to identify the data assets that can contribute to achieve the desired business outcomes. A governance charter should be created to detail the coordination and collaboration needed across state agencies to achieve these outcomes. A governance dashboard to measure and report the success of this initiative will provide the needed visibility and transparency across the enterprise for data governance.
- Adopt Zero Trust Architecture. President Joe Biden's May 12, 2021 executive order on improving the nation's cybersecurity requires federal agencies to advance the adoption of zero trust architecture. This is the answer to risks created by an "implicit trust" model (discussed in the key findings). The growth of ransomware attacks nationally, coupled with cloud adoption and the transition to hybrid (remote) workforce requires the state of Washington to accelerate adoption of a Zero Trust Architecture to improve our security posture and increase our cyber-resiliency. Our data, information technology systems and infrastructure will be much better protected with this approach. Our ecosystem will be better positioned to prevent a security incident or compromise from becoming a full-scale data breach by making both the attackers' life harder and giving state defenders more time and ability to react.
- Implement Enterprise Identity and Access Management. A robust Identity and Access Management (IAM) solution is a key prerequisite for the success of Zero Trust Architecture adoption. This foundation ensures that only the right people or machines have access to the appropriate assets for approved reasons, while keeping unauthorized access and fraud at bay. An effective IAM solution would greatly enhance the digital experience for Washingtonians accessing state government services while securing access to applications, services and data that face an onslaught of fraudulent activity. The plethora of privacy regulations and the sophistication of fraud activity experienced in Washington state underscores the need for an IAM solution architected for our modern digital environment.
- Modernize Security Operations. To improve visibility (discussed in Key Finding 2), the state of Washington needs to adopt modern, enterprise methods of data collection and analysis that can improve detection capabilities against more elusive attacks across our large enterprise. The state needs to partner with service providers who can accelerate performance and offer more proven, mature, and advanced capabilities. To reduce the mean time to detect and respond to incidents, the state needs to augment its operations with security monitoring, alerting, and remediation automation to enhance existing capabilities and move from reactive to a proactive security posture. The state's modernization efforts need to define metrics that measure the effectiveness of the state's security efforts. To be effective, these modernization efforts must be able to collect necessary data at an enterprise level from all systems, devices and applications utilized by all agencies. Agency participation is key. The state also must proactively find gaps in its detection and operational readiness through rigorous threat hunting, controls validation and penetration testing.

- **Establish an Enterprise Security Risk Management program.** An Enterprise Security Risk Management Program helps identify, evaluate and mitigate the likelihood and/or impact of security risk to the agency. This program allows risks to be quantified and prioritized in the context of the agency's mission and helps security professionals advise program owners in the process of making security risk management decisions that will in turn advance the overall mission of the agency This method allows enhanced partnership between the security professionals, program leaders and the agency leaders. This program will provide the following business outcomes:
    a. Identification and prioritization of agency assets. Assets will be prioritized in the context of the agency's mission and in the context of government services.
    b. Risk prioritization. Not all risks have the same business impact. Risks need to be prioritized based on the asset value and the value of this asset to the overall enterprise.
    c. Risk mitigation. This program will establish a process to mitigate the risks by starting with the most serious security threats and risks to the business of the agency.
    d. Process for continuous improvement. Risk management is a continuous process to help an agency to steadily improve its security posture. Risks needs to be continuously mitigated to ensure the security risks are continuously minimized while advancing the agency's mission.

# Section Two: Privacy

## Adherence to Privacy Principles

The foundation for modern privacy principles was formed decades ago with the development of fair information practice principles.[1] Since then, variations have been explicitly or implicitly included in virtually all significant privacy laws. Examples include the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Consumer Privacy Act and Europe's General Data Protection Regulation. They are also recognized in standards articulated by federal agencies and international organizations including the Federal Trade Commission, the Organization for Economic Co-operation and Development, and the United Nations. Although each variation has significant overlap, there is not a specific version uniformly recognized as authoritative.

One of the duties explicitly assigned to the OPDP by statute is to "articulate privacy principles and best practices."[2] Public agencies have an obligation to handle personal information responsibly and consistently with the law. Appropriate principles can help guide agency practices and decisions to maintain public trust. After extensive research and review, together with consideration of Washington culture and agency needs, OPDP drafted the Washington State Agency Privacy Principles (WSAPP) and distributed them to agencies for comment in July 2020. OPDP consulted with agencies, incorporated stakeholder feedback and finalized the principles in October 2020.


The Washington State Agency Privacy Principles are:

- Lawful, fair and responsible use.
- Data minimization.
- Purpose limitation.
- Transparency & accountability.
- Due diligence.
- Individual participation.
- Security.

Each principle is further defined together with a description of implementation. These principles are intended to be a high-level guide for agencies to follow when handling personal information about Washington

[1] *See, e.g.*, International Association of Privacy Professionals, *Fair Information Practice Principles*, https://iapp.org/resources/article/fair-information-practices/ (last accessed November 2, 2021).

[2] RCW 43.105.369(3)(c).

residents. They foster best practices and are scalable and flexible depending on the agency and the type of information and laws that apply to an agency's data.

Articulating and publishing the WSAPP is an important step, but it is only the beginning to implementation and adherence by agencies. There are several ways to advance use and promote adherence. Several are already underway including:

### Communication Tool:

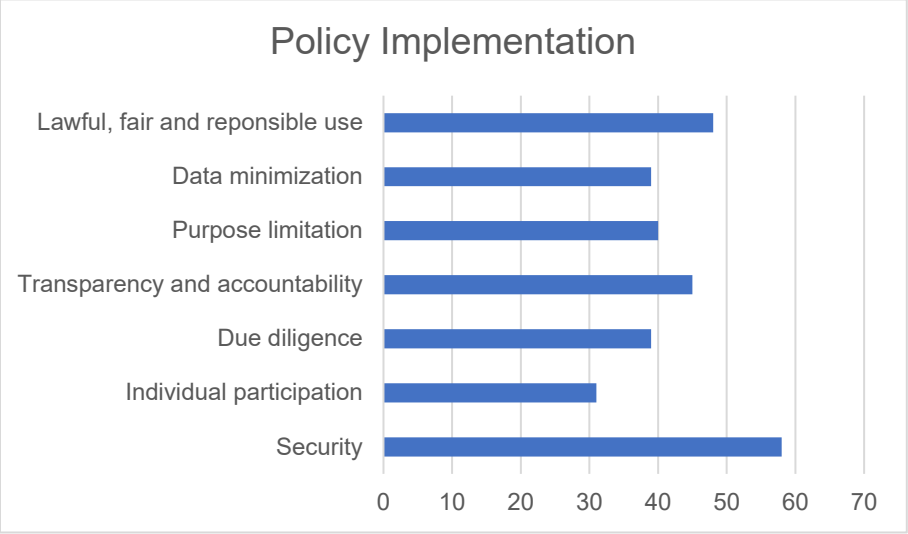
The WSAPP serve as a common language to discuss, consider and escalate matters related to personal information. For OPDP, this common language helps prioritize resource development and outreach efforts. And it provides helpful context to show agencies why tools, resources and presentations are important. For example, OPDP's breach assessment tool and data breach notification webinar are directly related to Transparency & Accountability, and its data request template is directly related to due diligence.

For agencies, the principles are easily understood shorthand for somewhat complicated topics. Broad concepts such as data minimization or purpose limitation may prompt inquiries or concerns sooner than relying on formal policies, which are less universally understood and may have blind spots. Relying on principles rather than formal policies helps shift thinking from compliance to doing the right thing.

### Policies and Processes:

Although formal policies and processes have their limitations (they can be dense, misunderstood, and neglect unforeseen circumstances) there is value in including privacy principles in formal policies. Doing so takes deliberate thought about how the principles interact with an agency's core functions, demonstrates maturity, and shows staff how seriously the agency takes privacy. It also documents expectations and creates formal authority to take tough steps to protect personal information, such as saying no to an external request for information or taking disciplinary action against an employee or contractor.

In OPDP's 2021 privacy assessment survey, 71 agencies indicated (see chart below) they maintain some type of personal information and many of those agencies indicated they have at least some of the concepts from the WSAPP as part of their internal policies:




To encourage further adoption and help agencies on their privacy maturity journeys, OPDP is working on a set of model policies based on the privacy principles. These policies can help agencies review and update

existing policies with key concepts or be used in their entirety by agencies without internal resources to create policies from scratch. OPDP's policies are expected to be published and available for use in winter 2021-2022. Almost all agencies indicated in their survey response that they are somewhat or very interested in model privacy policies to implement privacy principles.

### Training and Awareness

The fact that the WSAPP were published is of little use if employees are not aware they exist. Broad awareness and understanding improves the chances of consistent application and better decisions about how state agencies collect, maintain and share personal information. In addition to its routine outreach efforts and referencing the WSAPP whenever possible, OPDP is in the process of developing basic privacy training that will be available and accessible online for all state employees. The training will go over the basics of identifying and protecting personal information, and specifically highlight the WSAPP. Like model privacy policies, almost all agencies indicated in their privacy assessment survey responses that they are somewhat or very interested in basic privacy training for all staff.

### Workforce Development

Increasing the number and expertise of employees with privacy as part of their official duties is one of the best ways to scale adoption of privacy principles and other best practices across the state. These employees are inherently better situated to understand agency needs, implement best practices and advocate for sound decisions impacting personal information than the central Office of Privacy and Data Protection. The number of agencies with dedicated privacy staff is small but growing, and new staff are often in the position of building from the ground up. To help existing privacy staff expand their skillset and get new staff up and running, the OPDP is developing a privacy professionals bootcamp program expected to be launched by end of 2022.

This work will have the biggest impact if agencies continue to grow their internal privacy capacity. At a minimum, each agency that maintains personal information should have a designated privacy contact, regardless of whether privacy is the person's full-time job, to increase adoption and improve consistent messaging across the state. An increase in capacity can also have tangible benefits when responding to security incidents. Early involvement of staff with privacy expertise can help identify issues, deploy appropriate mitigation efforts, and save time and money complying with legal requirements.

### Privacy Impact Assessments, Frameworks and Maturity Models:

Incorporating privacy principles into formal assessments, program requirements or metrics is another important tool to increase adherence and implementation. OPDP is in the process of developing privacy impact assessments to examine and mitigate the privacy impacts of major state IT projects involving personal information. The tool, which is currently in draft form, is structured around the WSAPP. Privacy principles can also be incorporated into privacy frameworks and maturity measurements discussed later in this report. Doing so ensures meaningful adoption and accountability for implementation.

# Privacy Best Practices

The privacy landscape is constantly shifting:

- The regulatory environment is evolving from a patchwork of sectoral laws and self-regulation toward comprehensive privacy laws.
- Technological advances are enabling new ways to accumulate and use information, which can lead to societal benefits but also pose privacy risks.
- People are increasingly aware of data breaches, questionable data handling practices, and other risks to their privacy. As a result, their expectations for how their information is used, managed and shared are changing.
- The development of privacy as a professional discipline and as an important component of agency infrastructure is still relatively new.

In this environment, what is appropriate today may conflict with a new law enacted tomorrow. Or a completely legal and well-intentioned data use may conflict with people's expectations of how their information will be used. Laying a foundation for privacy best practices can help organizations make sound decisions and adapt as requirements and expectations change.

When implementing foundational privacy best practices, an organization should consider applicable regulations, frameworks and maturity models. Although there are not always clear lines between these categories, it is helpful to understand and consider them discretely.

## Laws and Regulations:

Many agencies have specific laws and regulations they must comply with. One key attribute that distinguishes these laws and regulations from frameworks or maturity models is compliance. Success is often determined by binary measurement against predefined criteria or requirements.

Relative certainty and predictability are the most attractive parts of a compliance-based approach to privacy. For that reason, even when there are not specific laws or regulations that apply, an agency may voluntarily seek privacy policies or standards to comply with. Compliance is recommended, and laws and regulations should be followed when they apply. But as with cybersecurity, compliance alone does not necessarily mean better privacy and data protection. For example, a law might not:

- Establish strong enough protections to meet people's expectations.
- Contemplate changes in technology and business practices.
- Account for an organization's specific mission or cultural context.

In these scenarios, there can be a gap between compliance and appropriate data protection controls. For this reason, compliance with laws and regulations is only one piece of effective privacy practices.

**Following Laws & Regulations**

+ Compliance

+ Relative Certainty

- Gaps

- Insufficient guidance to operationalize

Privacy laws and regulations can be comprehensive or target specific industry sectors like health, education or finance (sectoral laws). The defining characteristic of a comprehensive privacy law is that it applies generally to all types of information in the public and private sector. This differs significantly from the sectoral approach in the United States, where the legal protections that apply vary significantly depending on the jurisdiction, industry and type of information involved.

Two examples are provided below. The General Data Protection Regulation (GDPR) in Europe is the most widely known example of a comprehensive privacy law. In contrast, the Health Insurance Portability and Accountability Act of 1996 (together with its implementing regulations, HIPAA) in the United States is an example of a sectoral law that applies only to certain types of information, gathered for specific purposes, by certain types of organizations. Each example sets out a regulatory framework and not necessarily a privacy program framework.

### *General Data Protection Regulation*

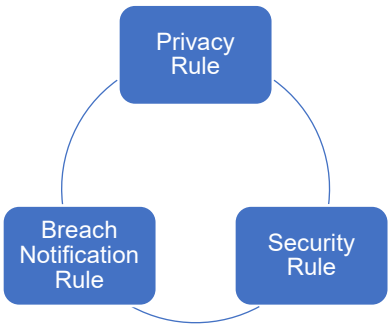
The European Union's GDPR passed the European Parliament in 2016 and become fully effective in May 2018.[3] In broad terms, the GDPR applies to all organizations that have a presence in the EU, store data in the EU, or target individuals in the EU (including through e-commerce).[4] Key pieces include:

- Requirements for processing data.
- Individual rights.
- Security breach notification.
- Designation of data protection officers.
- Sanctions (up to 4 percent of worldwide revenues).
- Rules and restrictions for international data transfers.

Because of its broad scope, the GDPR sets important protections for personal information in Europe and around the world. It codified many of the basic concepts and definitions that are now used to debate and enact privacy protections in the United States and around the world. For example, it includes core definitions for personal data, data processor, data controller, and data subject that serve as a helpful reference point and is one example of a law that explicitly includes fair information practice principles.[5]

### *Health Insurance Portability and Accountability Act of 1996*

HIPAA was originally passed in 1996 and its implementing regulations went into effect in the early 2000s.[6] It has been updated periodically, most notably by the Health Information Technology for Economic and Clinical Health Act in 2009.[7]




As suggested by its title, privacy was not the primary focus of the original act. It was intended to improve the portability and accountability of health insurance coverage and includes important administrative simplification and transactions rules. As concepts of privacy have become more central to people's everyday lives, HIPAA has become synonymous with health care privacy. Three HIPAA rules together form the basis for the privacy and confidentiality of health care information: The Breach Notification, Privacy, and Security Rules.

---

[3] What is GDPR, the EU's new data protection law?, https://gdpr.eu/what-is-gdpr/, (last accessed November 3, 2021).

[4] Does the GDPR apply to companies outside the EU?, https://gdpr.eu/companies-outside-of-europe/, (last accessed November 3, 2021).

[5] GDPR, Art. 5.1.

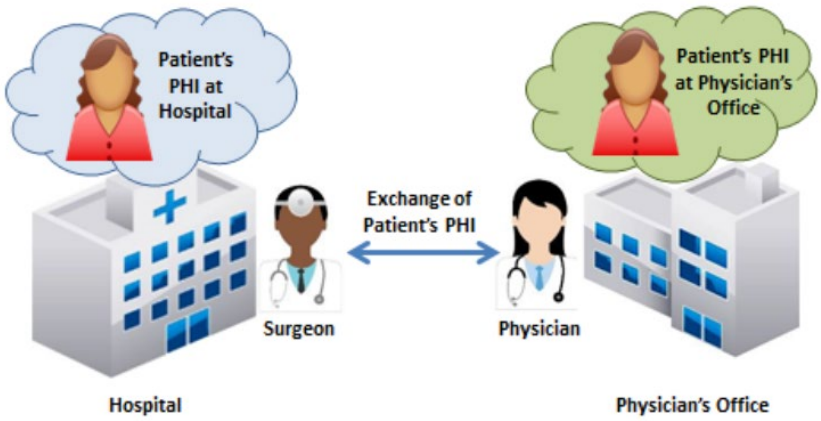
[6] HIPAA Journal, *HIPAA History*, https://www.hipaajournal.com/hipaa-history/, (*last accessed November 3, 2021*).

[7] *Id.*

These three rules constitute the most comprehensive implementation of fair information practice principles amongst federal United States privacy laws. For example, they include explicit requirements for security safeguards, data minimization, privacy notices, individual rights of access, and accountability when a data breach occurs. HIPAA is also notable for being frequently misunderstood to protect all health information. It is, in fact, limited to protecting certain types of information in certain settings. More specifically, it applies to protected health information held by covered entities and their business associates.

Protected health information (PHI) is identifiable information that is related to a person's health, health care, or payment for health care. Covered entities include health plans, health care clearinghouses, and health care providers that conduct electronic transactions. Business associates are contractors (or subcontractors) providing services for or on behalf of covered entities, or creating, receiving, maintaining or transmitting PHI. This scope effectively limits HIPAA's applicability to the closed universe of a person, their health care providers, health plans and contractors of their providers and plans.

For example, this image shows a typical exchange between a surgeon and treating physician. In this scenario, HIPAA applies to both doctors and PHI remains protected after it is shared between them.[8]




HIPAA offers no protections in most other situations, such as when a person shares their own health information with an employer or school (although other protections may apply in those situations). Recently there is emerging awareness that it also does not apply to a significant amount of health information gathered by wearable devices or shared for vaccine verification purposes.[9]

[8] U.S. Department of Health and Human Services Office for Civil Rights, Permitted Uses and Disclosures: Exchange for Treatment, https://www.hhs.gov/sites/default/files/exchange_treatment.pdf (last accessed November 3, 2021).

[9] U.S. Department of Health and Human Services Office for Civil Rights, HIPAA, COVID-19 Vaccination, and the Workplace, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-covid-19-vaccination-workplace/index.html (last accessed November 3, 2021).

## Frameworks

Unlike laws and regulations, which set data protection requirements, privacy frameworks provide the structure and basis to implement appropriate privacy practices and operationalize a privacy program. Privacy frameworks are not legally mandated, but they can typically be mapped to applicable legal requirements to ensure compliance.

**Using Frameworks**

Pros:

- Flexibility.
- Organization-specific roles & responsibilities.

Cons:

- May be misapplied.
- Not intrinsically tied to legal requirements.

Mapping to applicable legal requirements is one example of how frameworks are applied in an organization-specific way. Based on an organization's types of information, risk profile and resources, they may be applied in part or in whole. They can be applied in the way that best suits the organization's own culture and existing structure. That flexibility also leads to the possibility of applying the framework in a way that is too lenient or too conservative, thereby resulting in ineffective or inefficient privacy practices.

In the United States, one leading privacy framework is the relatively new NIST Privacy Framework. Other examples of frameworks include the Organization for Economic Co-operation and Development's Privacy Guidelines and the International Organization for Standardization's ISO/IEC 29100.

### NIST Privacy Framework:

The NIST Privacy Framework, published for the first time at the beginning of 2020, is relatively new. But it has gained traction-based alignment to the NIST's existing cybersecurity footprint. The stated goal is flexibility to address diverse privacy needs:

> *Deriving benefits from data while simultaneously managing risks to individuals' privacy is not well-suited to one-size-fits-all solutions. Like building a house, where homeowners make layout and design choices while relying on a well-engineered foundation, privacy protection should allow for individual choices, if effective privacy risk mitigations are already engineered into products and services. The Privacy Framework – through a risk- and outcome-based approach – is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and organizations, and stay current with technology trends, such as artificial intelligence and the Internet of Things.*[10]


[10] NIST Privacy Framework, p.i https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

Like the NIST Cybersecurity Framework, the Privacy Framework is made up of the Core, Profiles, and Implementation Tiers.

The Core, as its name implies, is the foundation for the Privacy Framework. It includes a set of activities and outcomes that are increasingly granular. It begins with five key functions. The Functions (see below) are structured like the NIST Cybersecurity Framework and designated with a "P" to differentiate them from the similarly named cybersecurity functions.

The five key functions in the Privacy Framework are:

Identify-P – Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

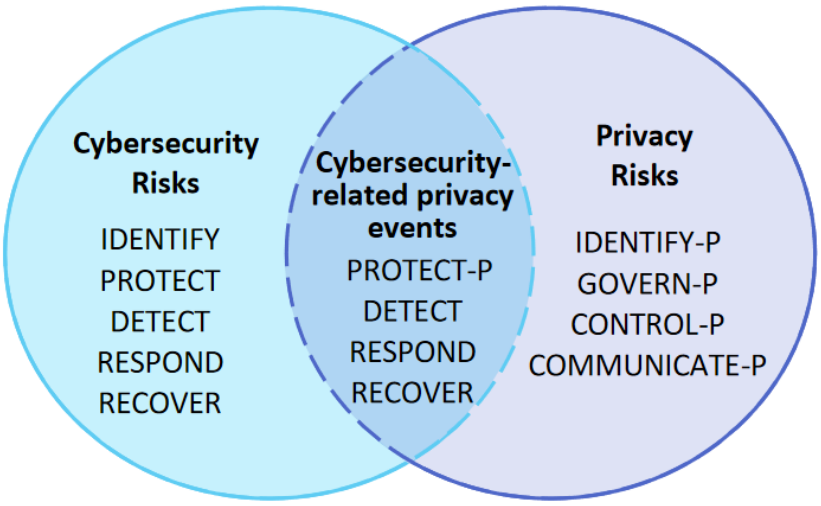
Govern-P – Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

Control-P – Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

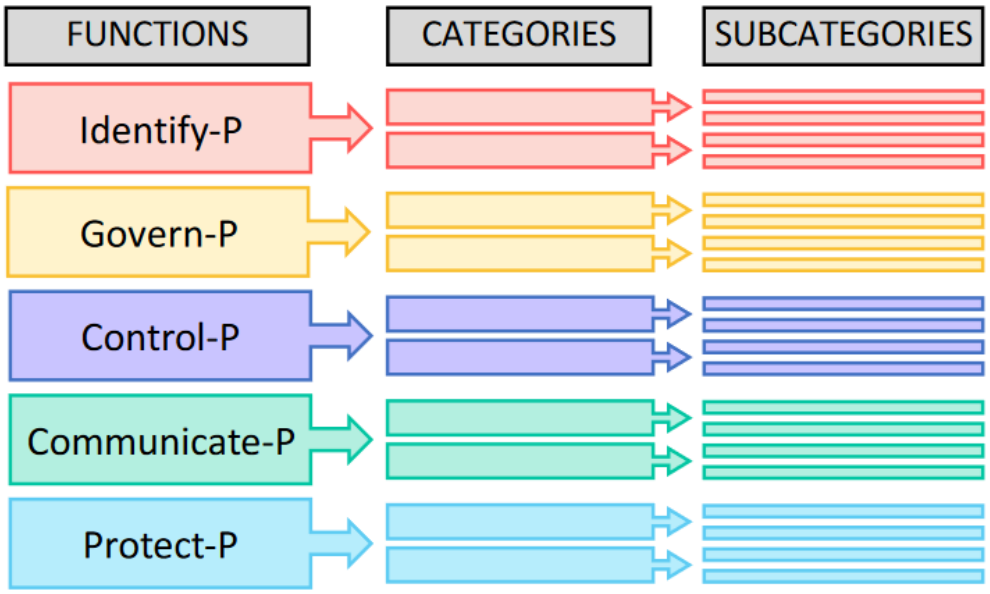
Communicate-P – Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.

Protect-P – Develop and implement appropriate data processing safeguards.

The structural similarity to the NIST Cybersecurity Framework allows a cohesive privacy and security framework for organizations implementing both. The image below uses these functions to show the overlap between cybersecurity risks, privacy risks, and cybersecurity-related privacy events.



The functions are further divided into categories and subcategories. The Categories and Subcategories are more discrete outcomes that help organizations implement the appropriate activities to perform each function.

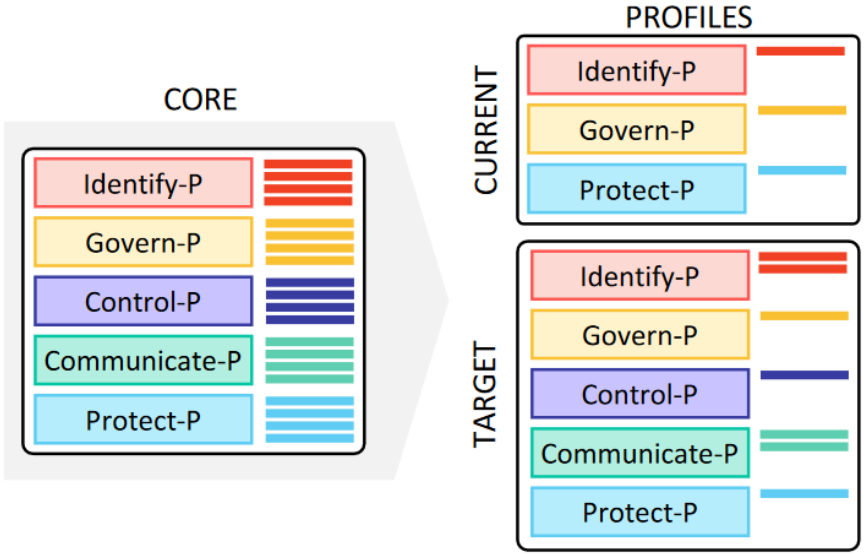



While the Core is the complete menu of functions, categories and subcategories, profiles are a specific selection. Two essential types of profiles are a Current Profile and Target Profile. A current profile includes the categories and subcategories that are already in place. A target profile includes the categories and subcategories an organization wants to have in place. Creating both allows gap analysis to improve internal privacy efforts. The Target Profile can also be used for external communication, such as by sharing with potential vendors as minimum requirements in a competitive procurement. There are no prescribed profile templates. Rather, an organization selects the items based on its own requirements, which may include its mission, privacy values, risk tolerance, resources and legal requirements.

Implementation Tiers, on the other hand, represent the progression of how an organization manages privacy risks. They are used as benchmarks to facilitate communication, and range from Tier 1 to Tier 4:

- Tier 1 – Partial
- Tier 2 – Risk-Informed
- Tier 3 – Repeatable
- Tier 4 – Adaptable

Importantly, not all organizations need to progress through all four tiers. Ultimate success is based on achieving the items in a Target Profile – not by progressing to Tier 4.



# Maturity Models

Maturity models help an organization measure against the expectations and standards established by applicable laws and selected privacy framework. They add a quantitative measurement so that an organization can determine not just what it needs or wants to do, but also how well it is doing it. As with privacy frameworks, it is not a one-size-fits-all approach and many factors will influence an organization's desired maturity level.

## *GAPP Privacy Maturity Model*

One widely used articulation of fair information practice principles is the American Institute of Certified Public Accountants' (AICPA) Generally Accepted Privacy Principles (GAPP).[11] In addition to articulating 10 privacy principles, the AICPA published a Privacy Maturity Model in 2011.[12]

There are five maturity levels in the model:

1. Ad hoc: Procedures or processes are generally informal, incomplete, and inconsistently applied.
2. Repeatable: Procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.
3. Defined: Procedures and processes are fully documented and implemented and cover all relevant aspects.
4. Managed: Reviews are conducted to assess the effectiveness of the controls in place.
5. Optimized: Regular review and feedback are used to ensure continuous improvement towards optimization of the given process.

The model includes 73 criteria, which are each under the umbrella of one of the ten articulated principles in the GAPP. Each criterion includes a description of the measurement, as well as guidance on determining the organization's current maturity from ad hoc to optimized.

| GAPP - 73 CRITERIA | CRITERIA DESCRIPTION | MATURITY LEVELS | | | | |
|---|---|---|---|---|---|---|
| | | AD HOC | REPEATABLE | DEFINED | MANAGED | OPTIMIZED |
| **MANAGEMENT (14 criteria) cont.** | **The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.** | | | | | |
| **Personal Information Identification and Classification (1.2.3)** | **The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity's privacy and related security policies and procedures.** | The identification of personal information is irregular, incomplete, inconsistent, and potentially out of date.<br>Personal information is not adequately addressed in the entity's privacy and related security policies and procedures.<br>Personal information may not be differentiated from other information. | Basic categories of personal information have been identified and covered in the entity's security and privacy policies; however, the classification may not have been extended to all personal information. | All personal information collected, used, stored and disclosed within the entity has been classified and risk rated. | All personal information is covered by the entity's privacy and related security policies and procedures. Procedures exist to monitor compliance.<br>Personal information records are reviewed to ensure appropriate classification. | Management maintains a record of all instances and uses of personal information. In addition, processes are in place to ensure changes to business processes and procedures and any supporting computerized systems, where personal information is involved, result in an updating of personal information records. Personal information records are reviewed to ensure appropriate classification. |

[11] Although still commonly referred to as GAPP, the AICPA updated the title of its privacy principles to the Privacy Management Framework in 2020. https://us.aicpa.org/interestareas/informationtechnology/privacy-management-framework, (*last accessed November 3, 2021*).

[12] https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf

Using these criteria can help an organization determine current state of a program or initiative, prioritize efforts or benchmark against other similarly situated organizations. An organization should take care to determine which level of maturity is appropriate for each criterion.

### Kuma's Privacy Maturity Approach:

At the beginning of 2021, OPDP began working with privacy and security consultant Kuma,[13] which is supporting many of OPDP's ongoing projects and initiatives. Kuma has created its own maturity model to help organizations improve their ability to make risk-informed privacy decisions.

The Kuma approach begins with five dimensions of a privacy program:

- Governance.
- Policy.
- Training and awareness.
- Data classification and IT assets.
- Data breach preparedness.


Each of those five dimensions is then evaluated using three metrics:

- Maturity refers to the level of development. A completely mature organization no longer needs to develop or expand.
- Saturation refers to the degree to which workforce members are aware of, understand and embody the policies and practices that apply to their work.
- Performance refers to individualized metrics to evaluate progress toward specific goals or objectives.

[13] https://kuma.pro/about/

## Privacy Recommendations

Compared to cybersecurity, privacy is a more federated and newer discipline for state agencies. Ultimately, agencies with a significant amount of personal information should implement privacy frameworks and maturity models to ensure they are not just complying with legal requirements, but also taking additional steps to identify gaps and appropriately protect sensitive information about Washington residents. While agencies have made significant progress in implementing best practices and improving the state's privacy maturity. A higher level of maturity, including formal adoption of privacy frameworks and privacy maturity models, is likely not attainable without additional investments in OPDP and agency privacy programs.

There are many additional steps OPDP, and state agencies can take to continue to improve privacy practices and adhere to privacy principles including:

- OPDP should develop additional training and awareness tools that incorporate the WSAPP and are tailored to address the greatest privacy and data protections risks.
- OPDP should ensure WSAPP are incorporated into new resources, such as privacy impact assessment templates.
- OPDP should continue to cultivate a community of privacy professionals to share best practices and promote professional development through a privacy professionals bootcamp program.
- OPDP should publish privacy impact assessment templates and agencies should use them to review privacy impacts as part of existing review processes for major IT projects that involve personal information.
- Agencies that hold personal information should continue to invest in their privacy programs. This includes at a minimum, having a designated privacy contact even if privacy is not that person's full-time job.
- Agencies should make training and awareness activities mandatory for staff who have access to personal information and consider making it mandatory for all staff.
- Agencies should implement formal privacy policies that incorporate the WSAPP.

# Section Three: Data Sharing Agreement Best Practices

Chapter 291, Laws of 2021 includes two sections that impose new requirements for data sharing agreements (DSAs) when sharing Category 3 or 4 information. Category 3 information is defined by OCIO Security Standard No. 141.10 as confidential information that is specifically protected from release or disclosure by law. It includes infrastructure and security information, proprietary information and personal information that is exempt from public disclosure. Category 4 information is confidential information requiring special handling that is specifically protected from disclosure, and for which there are especially strict handling requirements or serious consequences could arise from unauthorized disclosure. Examples include health or education records protected by federal privacy laws.

**Agency DSA Requirements**

RCW 39.26.340 – sharing with contractors.

RCW 39.34.240 – requesting from other agencies.

OCIO 141.10 – any sharing outside the agency.

RCW 39.26.340 requires state agencies to enter a written DSA before sharing Category 3 or higher information with a contractor. RCW 39.34.240 requires any public agency (including local jurisdictions) requesting Category 3 or higher information to "provide for a written agreement" with the other agency. Section 4 also states that this report should contemplate "model terms for data-sharing contracts."

These sections are consistent with the longstanding requirement in OCIO Policy Security Standard 141.10, section 4.2, that "[w]hen sharing Category 3 and above data outside the agency, an agreement must be in place unless otherwise prescribed by law." That requirement also includes core elements that should be included in data sharing agreements.

DSAs serve many functions, including:

- Ensuring appropriate protections for information to prevent incidents.
- Outlining responsibilities and mitigating agency impacts when an incident occurs.
- Documenting data flows to ensure an agency has a complete understanding of where its data is located.
- Forming a natural gate to vet relationships against privacy principles to ensure that the minimum amount of information is collected and shared, that uses are appropriately limited and that sharing is responsible and fair.

In practice, many agencies have worked hard for years to ensure appropriate agreements are in place when sharing Category 3 or 4 information. Recent cybersecurity events and the new statutory requirements have added urgency for many agencies to ensure appropriate agreements are in place. But there will always be room for improvement.

In 2019, the State Auditor's Office conducted an audit of agency contracting practices with information technology vendors. The underlying rationale for the audit was that even though the state "has little or no direct control over the security of its data" when hosted or managed by vendor applications, state agencies are "ultimately responsible for the state's data." The audit therefore analyzed areas to improve contract

terms to comply with security requirements, verify and monitor compliance, and protect the state in case of a data breach.

As part of its 2021 privacy assessment survey, OPDP asked agencies what steps they have taken to comply with the data sharing requirements in SB 5432 and what barriers to compliance they face. Many agencies have taken important actions to comply, such as:

- Reviewing or modifying existing DSA language.
- Creating new administrative controls such as policies that require agreements when information is shared.
- Entering new agreements to memorialize existing relationships.

Despite these steps, agencies may struggle when coming into compliance for myriad reasons, including:

- Timing constraints.
- Insufficient staffing resources to review data sharing relationships and/or execute agreements.
- Lack of existing approaches to data sharing oversite and approval.
- Additional education and training needed for staff.

Agencies also struggle with the terms of DSAs. In some cases, outside organizations dictate these terms giving agencies little control. Other agencies would prefer more standard templates to ensure consistency and appropriate requirements without extensive vetting.

To overcome these barriers, agencies should focus their efforts into three main categories:

- Identify and vet all situations where a DSA is necessary.
- Develop and implement appropriate DSAs.
- Ensure there is an adequate monitoring process to verify commitments to protect information are followed.

## Identify

The first step in protecting information with appropriate DSAs is identifying all instances where data is being shared. Although this seems straightforward, data sharing is often oversimplified to only include situations where new data extracts are created and sent outside an agency, and sometimes to only include special situations (such as research) outside the normal course of an agency's core functions.

But data sharing is better understood as any act of making data available to third parties. This includes not just one-off data extracts, but also routine data transmissions, data hosting and system access. It encompasses routine sharing that is necessary for the agency to perform core functions, such as sharing with contractors, service providers and other public agencies.

There are many steps agencies can take to identify all relationships where a DSA is necessary, and that data sharing with a particular recipient is appropriate, including:

> Consider all ways third parties access information: Ensure that DSAs are considered regardless of how information is shared, which could include at least ad hoc sharing, sending routine extracts, data hosting or system access.

Log and track data sent outside of systems: As part of broader data governance efforts, agencies should understand all instances where information is being transmitted outside the agency via extracts or other means that do not involve system access. This information can then be compared against existing DSAs to identify gaps.

Build safeguards into existing processes: Agencies should consider how to build DSA gates into existing processes. For example, a question can be added to the contracting process to determine whether a relationship involves data sharing. Or service request tickets sent to a data team can include a check to ensure an agreement is in place prior to sharing outside the agency.

Create common intake tools: Creating tools to document new data sharing relationships or requests for data, such as OPDP's data request template can help ensure visibility, consistency and appropriate vetting.

Develop approval requirement: Agencies should consider who has authority to approve new data sharing relationships. The appropriate authority will vary according to agency needs and risks, but includes a range of options:

- Staff can make decisions based on established criteria. This option is scalable and allows agency flexibility but can create inconsistency and is more likely to lead to inappropriate sharing.
- Only certain staff can authorize data sharing, such as data stewards, appointing authorities or other staff with specific authority and knowledge of appropriate data uses. This option is somewhat scalable and increases accountability while keeping decisions close to subject matter experts who understand business needs. By pushing decisions to a smaller group of individuals, it creates greater opportunities for consistency. It requires a robust data governance structure to be fully implemented.
- New data sharing relationships are reviewed and approved by a committee. This option creates accountability, consistency and visibility across all an agency's data sharing. It requires strong data governance, involvement of subject matter experts and triage and prioritization to avoid backlogs.

Confirm security requirements: Agencies should develop appropriate controls to ensure information is only shared with organizations that are able to appropriately protect it. The appropriate standards will vary depending on the purpose of the agreement and the types of information involved, but could include audits, requiring certification of appropriate security practices or security design review.

## Implement

Unfortunately, there is not just one, single version of model terms that is appropriate for all circumstances. The appeal of a single model is obvious – a single agreement could be easily adopted at scale, making compliance achievable even with minimal resources. But examining the various circumstances that may require a data sharing agreement, and the core elements of an effective DSA, makes it clear that a completely out of the box solution is not feasible or recommended.

For example, an agreement may involve two parties or many. It may involve one party sharing with another party or bi-directional sharing. When a relationship involves system access, a DSA may include significant details about the precise people who may access information and processes for provisioning access, but

only a general description of the type of information in the system. An agreement to memorialize sharing a one-time data extract, on the other hand, may include exact details about the data cohort, individual data elements, the timespan the data covers, and the method of transmission, while including little information about the precise people who may use the data.

It is also not always the case that data sharing terms are included within a standalone DSA. In fact, the OPDP has received many questions from agencies concerned that they need to execute new DSAs even though data share terms are already part of other agreements, or that they need to execute a contract literally titled "Data Sharing Agreement." OPDP's guidance has consistently been that:

- "Data sharing agreement" has not been defined in statute.
- It is not always necessary to execute a standalone DSA or call it by any specific name.
- What matters is having appropriate data share terms incorporated in an agreement, whether it is standalone or part of a more comprehensive contract.

Despite the required flexibility for DSA language, there is an opportunity to improve agency practices with the creation of additional templates and guidance. To that end, OCS, OPDP and the AGO reviewed several contracts in use by different agencies to develop:

- A chart with the types of terms that should or could be included in a DSA. This chart (see below) includes a description of the term. It can be used to gain a general understanding of the types of information that should be included in a DSA or as a checklist to compare against existing agreements.
- More detailed Data Sharing Agreement Implementation Guidance that includes terms and their description, together with examples of appropriate terms. This guidance can help provide more information about how the amount of detail included may vary from contract to contract. This guidance is attached as Addendum A. It will be published to OPDP's website together with several examples of DSA templates.

It is important to note that although these terms are appropriate for most DSAs, the level of detail for each term may vary significantly from agreement to agreement. They are also not meant to ensure compliance with any set of laws and depending on the type of information an agency maintains, there may be additional required elements.

| Term | Explanation |
|---|---|
| ***Should include*** | |
| Purpose and specific authority for sharing. | Describe why the information is being shared and the specific authority for sharing it. Authority to share may come from a variety of places, including laws, contracts, funding requirements, or policies. When sharing with a vendor this may include a description of the agency function being facilitated by sharing the information. |
| A description of the data, including classification. | Describe the information being shared, including data classification. Include as much specificity as possible, but the level of detail is likely to vary significantly depending on context. For example, listing specific data elements may be appropriate for a one-time arrangement with a researcher, but impracticable for an agreement with a technology vendor that has access to a wide range of information. In some cases, it may be |

| | |
|---|---|
| | appropriate to execute an overarching agreement with more detailed schedules or attachments executed as needed. |
| Authorized uses. | Describe how the information may be used, including prohibited uses (e.g., for commercial purposes). When the agreement is with a contractor performing functions on behalf of an agency, authorized uses should typically be limited to those functions. |
| Authorized users or classes of users. | Describe the specific individuals or classes of individuals who may access the information. This may include subcontractors or other third parties, and any approval process for those subcontractors or third parties. |
| Protection of the data in transit if the arrangement involves transmission. | If the arrangement involves data transmission, describe how the information will be sent and how it will be protected in transit (e.g.: encryption). If the arrangement involves system access, explain how access will be provisioned. |
| Secure storage for data maintained outside the agency. | Describe storage and handling requirements, including applicable encryption at rest or other security requirements. |
| Data disposal. | Describe when and how the information will be destroyed or returned, including a mechanism to verify disposal is completed. |
| Backup requirements if applicable. | Include backup and recovery specifications when applicable, such as when the recipient is storing the copy of record. |
| Incident notification and response. | Describe incident response requirements if information is compromised. Include at least requirement to notify, timing, expenses, and roles and responsibilities. |
| Monitoring and enforcement. | Describe measures to monitor and enforce the agreement, including remedies for violations. Depending on risk profile and available resources, monitoring could include attestations, verification or audits. At a minimum, remedies should include the right to terminate and have information destroyed or returned. |
| Awareness and/or training. | Describe measures to ensure authorized users understand their responsibilities. Examples could include general privacy training or specific nondisclosure agreements for the shared information. |
| Compliance with additional relevant OCIO security requirements based on the type of data sharing. | Depending on the specific functions performed by the recipient, compliance with other OCIO security requirements may be required. |
| Any other requirements imposed by law, regulation, contract or policy. | Include any other specific data sharing requirements that apply to the information. For example, HIPAA includes specific requirements for contracts with business associates accessing protected health information on behalf of a covered entity. |
| ***Might include*** | |
| Term and termination. | Describe the effective term, which may end with a date or an event. Although not unique to DSAs, including an appropriate term provision ties directly into data minimization and purpose limitation. Appropriate termination provisions tie directly into adequate enforcement remedies. |
| Off-shore prohibition. | Include a prohibition on storing or sharing information outside of the United States when prohibited by law, contract or policy. Even when not formally prohibited, before allowing information to be stored outside of the United States consider the ability to protect the information and seek recourse in a foreign jurisdiction. Also consider the criticality and |

| | |
|---|---|
| | sensitivity of the information, including the impact of the loss of confidentiality, integrity or availability. |
| Cyber liability insurance. | Cyber liability insurance is a specific type of insurance coverage to protect an agency from the costs associated with a data breach or other cybersecurity issues. It is discrete from the commercial general liability requirements often included in agency contracts and the technology errors and omissions insurance that may be appropriate for contracts with IT vendors.<br><br>When sharing confidential information with outside vendors, agencies should require sufficient cyber liability coverage to protect the state in the event of an incident. The appropriate amount may vary depending on the type and amount of information being shared, and the amount of information from other organizations covered by the policy.<br><br>State agencies may have their own cyber liability insurance purchased through the Department of Enterprise Services. |
| Indemnification. | This term serves to compensate an agency for harm or loss arising in connection with a vendor or contractor's actions or failure to act. The intent is to shift liability away from an agency on to the indemnifying party. Generally, this term should be included in all vendor and contractor agreements. |
| Third party requests. | Consider including processes for handling requests for information from third parties. This may include court orders and subpoenas or the Public Records Act, particularly when sharing information with other public agencies. |
| Restrictions on disclosure or publication. | Some data recipients, such as researchers, may intend to publish data or analysis. Consider including publication procedures, such as de-identification standards or agency review prior to publication. |
| Other widely applicable contract terms. | There are many generic contract terms (i.e.: boilerplate) that may be appropriate for a DSA, that are not specific to the data sharing arrangement itself. Examples include governing law, severability, and order of precedence. These types of terms should be included when appropriate, and care should be exercised to ensure consistency when the DSA terms are used as an addendum or exhibit to another contract. |

## Monitor

Executing a DSA is not the end of appropriate third-party management. Agencies should also take steps to verify, monitor and enforce the terms of the agreement. Effective monitoring may include the tasks below and begins with selecting appropriate terms to include in the DSA:

**Assign responsibility within agency:** Agencies should assign appropriate roles and responsibilities as part of their data sharing responsibilities. For example, a contracts assistant may be the appropriate person to ensure nondisclosure agreements have been signed and returned. But they are likely not the appropriate person to understand the data itself, the appropriate business uses of the information, or the legal requirements that apply to the data.

**Contemplate compliance measurement:** Agencies should determine the level of compliance assurance needed, which could include things like reserving the right to audit, requiring third party audits, or gathering attestations. If an agency includes terms that require audits or attestations, it should ensure it has processes in place and capacity to verify compliance.

**Include enforcement controls:** Agencies should include appropriate enforcement controls in DSAs. In most cases, appropriate controls include at least the ability to stop sharing or terminate an agreement and may include the ability to impose sanctions when the agency has authority to do so.

**Certify disposal:** Agencies should implement a process to ensure data is securely destroyed or returned when a contract ends, or the data is no longer needed. This includes controls to identify when information should be destroyed or returned. It also includes assigning responsibility to agency staff to ensure proper disposal has occurred through appropriate documentation and written assurances.

**Inventory data sharing agreements:** Just like agencies need to identify the situations where a DSA is in place, they also need to be able to identify existing DSAs. This can be difficult due to factors like inconsistent naming conventions or the fact that DSAs are sometimes standalone and sometimes part of larger agreements. The challenge can be overcome by requiring consistent naming conventions, appropriate tagging, maintaining agreements in a searchable contract management system, and/or designating an appropriate person to be responsible for the process.

# Data Sharing Agreement Recommendations

Executing appropriate DSAs is an essential piece of understanding where an agency's data is located. DSAs ensure appropriate protections are in place when outside entities receive or have access to agency confidential information. Agencies have taken many steps to ensure DSAs are in place, but there are additional steps that could help eliminate gaps where sharing is not documented and improve data sharing language where DSAs are in place.

- OCIO should update the required elements for a DSA in OCIO Security Standard 141.10, to reflect the chart on pages 26-28 of this report.
- The Data Sharing Agreement Implementation Guidance developed as part of this report should be published and promoted for agency use.
- Agencies should implement the controls listed in this report (pages 24-29) to ensure appropriate DSA practices, which may include creating checkpoints to verify when data is being shared, developing intake tools, formalizing data sharing approval processes, gaining assurances that appropriate security standards are being met and certifying destruction of data when a data sharing relationship ends.

# Contact

Questions regarding this report can be directed to:

Derek Puckett
Legislative Affairs Director
Washington Technology Solutions
Derek.Puckett@watech.wa.gov

WaTech
Washington Technology Solutions
*Washington's Consolidated Technology Services Agency*

# Data Sharing Agreement Implementation Guidance

December 2021, v.1

**Addendum A**

This guidance was created in collaboration between the Office of Privacy and Data Protection, the Office of Cybersecurity, and the Attorney General's Office as one piece of a privacy and cybersecurity best practices report required by ESSB 5432 (2021). It is intended to help agencies successfully implement appropriate data sharing agreements (DSAs) to protect confidential information.

Data sharing relationships take many forms. While this document is a resource that can help agencies assess options, it is not provided for the purpose of giving legal advice of any kind. This guide does not represent the legal opinion of any Washington state agency, including the Attorney General's Office. Readers should not rely on information in this guide regarding specific applications of the laws without seeking legal counsel.

## Data Sharing Agreement Requirements

Broad DSA requirements (in addition to requirements that may apply to specific agencies or specific types of information) exist for Washington state agencies in at least three places:

> RCW 39.26.340(1) states that "[b]efore an agency shares with a contractor category 3 or higher data, as defined in policy established in accordance with RCW 43.105.54, a written data-sharing agreement must be place." Within chapter 39.26 RCW, agency means office or activity of the executive or judicial branches of state government.
>
> RCW 39.34.240(1) states that "[i]f a public agency is requesting from another public agency category 3 or higher data . . . the requesting agency shall provide for a written agreement between the agencies . . . ." Within chapter 39.34 RCW, a public agency means any agency, political subdivision, or unit of local government; any state agency; any United States agency; any federally recognized tribe; and any political subdivision of another state.
>
> OCIO Policy #141.10 states that "[w]hen sharing Category 3 and above data outside the agency, an agreement must be in place unless otherwise prescribed by law." OCIO Policy #141.10 applies to executive branch agencies and agencies headed by separately elected officials.

Taken individually these requirements could conceivably be interpreted to create a patchwork of DSA mandates. But together they reinforce the best practice that an agency should typically enter DSAs when a person outside the agency receives or has access to confidential information. Entering into DSAs is also consistent with the Washington State Agency Privacy Principles. It is most obviously a core part of the due diligence principle, which requires exercising care when sharing information with third parties. DSAs also support the remaining principles by carrying forward the agency's own obligations as a trusted steward of information and are one part of ensuring an agency understands all the places where its data is located.


## Using this Document

This document includes 13 categories of contract terms that should typically be included in a DSA, and seven other terms that might be included depending on the nature of a specific scenario. Each section includes general guidance on implementation, together with example language when possible.



# Addendum A

There are core concepts that should typically be included in any agreement that contemplates data sharing, but there is no rigid requirement for a particular format or level of detail. The details of a particular data sharing relationship can significantly impact the overall structure of the agreement, the types of terms to include, the level of detail required and even whether a DSA is feasible at all. For example, when sharing a one-time extract with a researcher, it will be possible to list specific data elements and the specific persons authorized to access the information. When sharing with an IT vendor with broad access to agency data on an ongoing basis, such granularity is not possible.

Based on this variability DSAs may be:

- Standalone or part of a larger agreement.
- One-way or bidirectional.
- Very specific about data elements involved or provide a general description of information.

In determining the appropriate format for a particular relationship, agencies should feel empowered to exercise sound discretion and flexibility. In doing so, they should consider at least:

- The number of parties involved
- Whether sharing is one-way or bidirectional
- The frequency of sharing
- The types of information involved and whether specific legal requirements apply
- The scope of information involved
- The nature of the purpose for sharing
- The nature of the data recipient and the recipient's relationship with the agency

With these considerations in mind, the examples below can be used to create DSAs, or as a tool to review and strengthen existing DSAs. In doing so:

- Do not assume it is just a matter of selecting one option from each section. There may be multiple appropriate terms or none.
- Be ready to add content and narrative. For some terms the content is so situation-specific that templates are not possible.
- Understand that some terms overlap. For example, describing the purpose, appropriate uses, appropriate users, and methods of access do not necessarily need to be five separate contract terms.
- Exercise flexibility only when appropriate for specific terms. A relationship with an IT vendor with broad access to information may warrant flexibility regarding the description of data, but not security requirements.

## Should include – Purpose and specific authority for sharing

*Describe why the information is being shared and the specific authority for sharing it. Authority to share may come from a variety of places, including laws, contracts, funding requirements, or policies. When sharing with a vendor this may include a description of the agency function being facilitated by sharing the information.*

**Examples**

| | |
|---|---|
| Purpose of the agreement itself | The purpose of this DSA is to provide terms and conditions under which [Agency] will allow the restricted use of its Confidential Information to the Receiving Party, and under which the Receiving Party may receive and use the Confidential Information. This DSA ensures that [Agency] Confidential Information is provided, protected, and used only for purposes authorized by this DSA and state and federal law governing such use. |
| Purpose of sharing and authority to share | The Confidential Information to be shared under this DSA is shared . . . [Explain the purpose and authority for sharing. If the information is shared to help the agency fulfill its statutorily authorized functions, cite to those statutes. If the sharing is specifically allowed or required by statute, rule or other authority, cite to that authority.] |

## Should include – Description of the data, including classification

*Describe the information being shared, including data classification. Include as much specificity as possible, but the level of detail is likely to vary significantly depending on context. For example, listing specific data elements may be appropriate for a one-time arrangement with a researcher, but impracticable for an agreement with a technology vendor that has access to a wide range of information. In some cases, it may be appropriate to execute an overarching agreement with more detailed schedules or attachments executed as needed.*

Examples

<table>
<tr><td>Appropriate definitions of protected information</td><td>“Personal Information” means information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, Social Security Numbers, driver license numbers, other identifying numbers, and any financial identifiers.<br><br>“Confidential Information” or “Data” means information that is exempt from disclosure under chapter 42.56 RCW or other federal or state laws. Confidential Information includes both Category 3 and Category 4 information including, but not limited to, Personal Information.</td></tr>
<tr><td>For broad sharing when data cannot be specifically defined</td><td>Data to be shared includes . . . .<br><br>[Describe the data with as much specificity as possible, including at least data classification and the circumstances when information is shared. Where it is not possible to describe specific elements, describing the purpose and processes for sharing provides helpful context].</td></tr>
<tr><td>When listing specific elements is possible</td><td>Data will be exchanged using the mutually agreed upon file layouts below.<br><br>i. Method of Access/Transfer: [describe how information is shared]<br><br>ii. Frequency of Data Delivery: [describe how often the information is shared]<br><br><table><tr><th>Element Name</th><th>Short Description</th><th>Length</th><th>Type</th><th>Data Descriptions and Usages</th></tr><tr><td></td><td></td><td></td><td></td><td></td></tr></table><br>[Customize table layout for column names appropriate for the type of data being shared. When sharing multiple extracts with a single recipient, agencies can document this information (and the purpose) for each extract as schedules or addendums]</td></tr>
</table>

| | |
|---|---|
| Data Classification as its own term | The State classifies data into categories based on the sensitivity of the data pursuant to the Security policy and standards promulgated by the Office of the state of Washington Chief Information Officer.<br><br>The Data that is the subject of this DSA is classified as indicated below:<br><br>☐ Category 1 – Public Information<br><br>Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.<br><br>☐ Category 2 – Sensitive Information<br><br>Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.<br><br>☐ Category 3 – Confidential Information<br><br>Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:<br><br>a. Personal Information about individuals, regardless of how that information is obtained;<br><br>b. Information concerning employee personnel records;<br><br>c. Information regarding IT infrastructure and security of computer and telecommunications systems;<br><br>☐ Category 4 – Confidential Information Requiring Special Handling<br><br>Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:<br><br>a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements;<br><br>b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions. |
| Requirement to specifically notify when Confidential Information is being shared | Agency will notify [Receiving Party] if they are providing Confidential Data. |

## Should include – Authorized uses

*Describe how the information may be used, including prohibited uses. When the agreement is with a contractor performing functions on behalf of an agency, authorized uses should typically be limited to those functions.*

**Examples**

| | |
|---|---|
| General limitation on permitted uses | This Agreement does not constitute a release of Confidential Information for the Receiving Party's discretionary use and may be accessed and used only to carry out the purposes described in this DSA. Any ad hoc analyses or other use of the data, not specified in this DSA, is not permitted without the prior written agreement of [AGENCY]. |
| General limitation on permitted uses for non-vendors | The Receiving Party will not use, publish, transfer, sell, or otherwise disclose any Confidential Information gained by reason of this DSA for any purpose that is not directly connected with the purpose, justification, and permitted uses of this DSA, except:<br>(a) as provided by law; or<br>(b) with the prior written consent of the person or personal representative of the person who is the subject of the Data. |
| General limitation on permitted uses for vendors | The Contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Contract for any purpose that is not directly connected with Contractor's performance of the services contemplated hereunder, except:<br>(1) as provided by law; or,<br>(2) in the case of Personal Information, with the prior written consent of the person or personal representative of the person who is the subject of the Personal Information. |
| Prohibition on commercial or personal use | Receiving Party shall not access or use the Confidential Information for any commercial or personal purpose. |
| Prohibiting data linkage | The Confidential Information shared under this DSA may not be linked with other data sources without prior written agreement of [Agency]. |
| Allowing data linkage | The Confidential Information shared under this DSA may be linked with the following data sources: [*list sources*]<br>[*When allowing data linkage, consider possible impacts such as whether the combined data will be shared with other parties, and whether Agency data will remain identifiable after combination*] |
| Prohibition on data modifications | The Receiving Party is not authorized to update or change any Data in [Agency system], and any updates or changes will be cause for immediate termination of this DSA. |

## Should include – Authorized users or classes of users

*Describe the specific individuals or classes of individuals who may access the information. This may include subcontractors or other third parties, and any approval process for those subcontractors or third parties.*

Examples

| | |
|---|---|
| Appropriate definitions of Contractor or Receiving Party | "Contractor" means the individual or entity performing services pursuant to this Contract and includes the Contractor's owners, members, officers, directors, partners, employees, and/or agents, unless otherwise stated in this Contract. For purposes of any permitted Subcontract, "Contractor" includes any Subcontractor and its owners, members, officers, directors, partners, employees, and/or agents.<br><br>"Receiving Party" means the entity that is identified on the cover page of this DSA and is a party to this DSA, and includes the entity's owners, members, officers, directors, partners, trustees, employees, and Subcontractors and their owners, members, officers, directors, partners, trustees, and employees. |
| General prohibition on sharing with unauthorized users | Receiving Party shall not disclose, in whole or in part, the Data provided by [Agency] to any individual or entity, unless this Agreement specifically authorizes the disclosure. Data may be disclosed only to persons and entities that have the need to use the data to achieve the stated purposes of this Agreement. |
| General designation of authorized users | Receiving Party must identify:<br><br>A. Those persons or classes of persons in its workforce who need access to Confidential Information to carry out their duties; and<br><br>B. For each such person or class of persons, the types of information to which access is needed and any conditions appropriate to such access. |
| Procedures to limit access | Receiving Party must implement policies and procedures that limit the Confidential Information disclosed to such persons or classes of persons to the amount reasonably necessary to achieve the purpose of the disclosure as described in this DSA. |
| Subcontractor approval requirements | The Receiving Party will not enter into any Subcontract without the express, written permission of [Agency], which will approve or deny the proposed subcontract in its sole discretion. If Data access is to be provided to a Subcontractor under this DSA it will only be for the specific purpose and uses authorized by [Agency] and the Receiving Party must include all of the Data security terms, conditions and requirements set |

| | |
|---|---|
| | forth in this DSA in any such Subcontract. In no event will the existence of the Subcontract operate to release or reduce the liability of the Receiving Party to [Agency] for any breach in the performance of the Receiving Party's responsibilities.<br><br>This DSA does not constitute a release for Receiving Party to share the Data with any third parties, including Subcontractors, even if for authorized use(s) under this DSA, without the third-party release being approved by [Agency] and identified in the Data Licensing Statement(s). |

## Should include – Protection of the data in transit if the arrangement involves transmission

*If the arrangement involves data transmission, describe how the information will be sent and how it will be protected in transit. If the arrangement involves system access, explain how access will be provisioned.*

Examples

| | |
|---|---|
| Transmission method | *[Describe how the information will be transferred, including applicable encryption protocols or other protections to ensure secure transfer]* |
| System access | The Receiving Party may request access to [Agency system] for up to [number of] Authorized Users under this DSA.<br><br>The Receiving Party must send the request for new users to [Agency contact]. Receiving Party must designate a Point of Contact to be the single source of access request for new users.<br><br>Receiving Party may not use shared User IDs and passwords for use with Confidential Information or to access systems that contain Confidential Information. Receiving Party must ensure that only Authorized Users access and use the system(s) in this DSA, use only their own User ID and password to access the system(s), and do not allow employees or others who are not authorized to borrow a User ID or password to access any system(s).<br><br>Receiving Party must notify [Agency] within 5 business days whenever an Authorized User who has access to the Data is no longer employed by the Receiving Part or whenever an Authorized User's duties change such that the user no longer requires access to the Data.<br><br>Receiving Party's access to the systems may be continuously tracked and monitored. [Agency] reserves the right, at any time, to terminate Data access for an individual, conduct audits of system(s) access and use, and to investigate possible violations of this DSA and/or violations of laws governing access to Confidential Information. |

## Should include – Secure storage for data maintained outside the agency

*Describe storage and handling requirements, including applicable encryption at rest or other security requirements.*

**Examples**

| | |
|---|---|
| General security statement | [Agency] shall take due care and take reasonable precautions to protect Agency's data from unauthorized physical and electronic access. Receiving Party certifies that it complies with the requirements of the OCIO 141.10 policies and standards for data security and access controls to ensure the confidentiality, integrity and availability of all data shared.<br><br>Receiving party will restrict access to Confidential Information by:<br><br>A. Allowing access only to staff that have an authorized business requirement to view the Confidential Information.<br><br>B. Physically securing any computers, documents, or other media containing the Confidential Information.<br><br>[*This language is not intended to encompass all appropriate security requirements*] |

## Should include – Data disposal

*Describe when and how the information will be destroyed or returned, including a mechanism to verify disposal is completed.*

**Examples**

| | |
|---|---|
| General disposal requirement | Upon request by [Agency], or at the end of the DSA term, or when no longer needed, Confidential Information/Data must be returned or destroyed using an Agency approved disposal method, except as required to be maintained for compliance or accounting purposes. Receiving Party will provide written certification of disposition using [certificate of disposal, attachment 1] |
| Disposal of paper records | Paper documents with Confidential Information may be recycled through a contracted firm, provided the contract with the recycler specifies that the confidentiality of information will be protected, and the information destroyed through the recycling process. Paper documents containing Category 4 information must be destroyed on-site through shredding, pulping, or incineration. |

## Should include – Backup requirements if applicable

*Include backup and recovery specifications when applicable, such as when the recipient is storing the copy of record. Appropriate language will depend on agency needs and the function being performed.*

## Should include – Incident notification and response

*Describe incident response requirements if information is compromised. Include at least requirement to notify, timing, expenses, and roles and responsibilities.*

Examples

| | |
|---|---|
| General notification requirement | The compromise or potential compromise of Confidential Information that may be a breach that requires notice to affected individuals under RCW 42.56.590, RCW 19.255.010, or any other applicable breach notification law or rule must be reported to the [Agency privacy contact] within one (1) business day of discovery. |
| Information to be provided | If the Receiving Party does not have full details about the incident, it will report what information it has and provide full details within 15 business days of discovery. To the extent possible, these initial reports must include at least:<br>A. The nature of the unauthorized use or disclosure, including a brief description of what happened, the date of the event(s), and the date of discovery;<br>B. A description of the types of information involved;<br>C. The investigative and remedial actions the Receiving Party or its Subcontractor took or will take to prevent and mitigate harmful effects and protect against recurrence;<br>D. Any details necessary for a determination of whether the incident is a breach that requires notification under RCW 19.255.010, RCW 42.56.590, or any other applicable breach notification law or rule.<br>E. Any other information [Agency] reasonably requests. |
| Requirement to mitigate | Receiving Party must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or [Agency]. |

| | |
|---|---|
| Notification | If notification to individuals must, in the sole judgement of [Agency], must be made Receiving Party will further cooperate and facilitate notification to required parties, which may include notification to affected individuals, the media, the Attorney General's Office, or other authorities based on applicable law.<br><br>At [Agency's] discretion, Receiving Party may be required to directly fulfill notification requirements, or if [Agency] elects to perform the notifications, Receiving Party must reimburse [Agency] for all associated costs. |
| Costs | Receiving Party is responsible for all costs incurred in connection with a security incident, privacy breach, or potential compromise of Data, including:<br><br>A. Computer forensics assistance to assess the impact of a Data Breach, determine root cause, and help determine whether and the extent to which notification must be provided to comply with Breach notification laws;<br><br>B. Notification and call center services for individuals affected by a security incident or privacy Breach, including fraud prevention, credit monitoring, and identify theft assistance; and<br><br>C. Regulatory defense, fines, and penalties from any claim in the form of a regulatory proceeding resulting from a violation of any applicable privacy or security law(s) or regulation(s). |
| Survival | Receiving Party's obligations regarding breach notification survive the termination of this DSA and continue for as long as Receiving Party maintains the Data and for any breach or potential breach, at any time. |

## Should include – Monitoring and enforcement

*Describe measures to monitor and enforce the agreement, including remedies for violations. Depending on risk profile and available resources, monitoring could include attestations, verification or audits. At a minimum, remedies should include the right to terminate and have information destroyed or returned.*

### Examples

| | |
|---|---|
| General right to monitor and audit | The Receiving Party agrees that [Agency] will have the right, at any time, to monitor, audit, and review activities and methods in implementing this Agreement in order to assure compliance. |



# Addendum A

| | |
|---|---|
| Alternative right to audit language | During the term of this DSA and for six (6) years following termination or expiration of this DSA, [Agency] will have the right at reasonable times and upon no less than five (5) business days prior written notice to access the Receiving Party's records and place of business for the purpose of auditing, and evaluating the Receiving Party's compliance with this DSA and applicable laws and regulations. |
| Third party audits | At [Agency's] request or in accordance with OCIO Security Standard No. 141.10, Receiving Party shall obtain third-party audits covering Data Security and Permissible Use. Receiving Party may cover both the Permissible Use and the Data Security Requirements under the same audit, or under separate audits. |
| Penalties | Any disclosure of Data contrary to this DSA is unauthorized and is subject to penalties identified in law. |

## Should include – Awareness and/or training

Describe measures to ensure authorized users understand their responsibilities. Examples could include general privacy training and/or specific nondisclosure agreements for the shared information.

**Examples**

| | |
|---|---|
| Employee awareness | The Receiving Party shall ensure that all staff with access to the data described in this Agreement are aware of the use and disclosure requirements of this Agreement and will advise new staff of the provisions of this Agreement.<br><br>[Agency] will provide an annual reminder to staff of these requirements.<br><br>[*Agencies may add to this language to require generic data handling training, or training specific to the agreement*] |
| Nondisclosure agreements | Individuals will access Data only for the purpose of this Agreement. Each individual shall read and sign [Agency confidentiality and non-disclosure agreement] prior to being granted access to the Data. The Receiving Party will retain a signed copy of [Agency confidentiality and non-disclosure agreement] in each employee's personnel file for a minimum of six years from the date the employee's access to the Data ends. The documentation must be available to [Agency] upon request. |

| | |
|---|---|
| | [*Agencies may modify how long these agreements must be maintained, or proactively collect signed copies prior to sharing information or granting access*] |

## Should include – Compliance with additional relevant OCIO security requirements based on the type of data sharing

*Depending on the specific functions performed by the recipient, compliance with other OCIO security requirements may be required.* [Specific security requirements will vary significantly based on the function being performed and agencies are expected to include these requirements as applicable]

### Examples

| | |
|---|---|
| General security statement | The Contractor shall protect and maintain all Confidential Information gained by reason of this Contract against unauthorized use, access, disclosure, modification or loss. This duty requires the Contractor to employ reasonable security measures in accordance with OCIO security standard 141.10 |
| Alternative general security statement | Receiving Party shall use appropriate safeguards to prevent the inappropriate use, disclosure and/or loss of Confidential Information. Receiving Party shall adopt reasonable and necessary administrative, technical and physical safeguards to ensure the confidentiality, availability and integrity of the Confidential Information. Receiving Party acknowledges that [Agency] is relying on the administrative, physical, and technical safeguards implemented by the Receiving Party in permitting access to Confidential Information subject of this Agreement. The Receiving Party represents and warrants that it has adopted, implemented, and shall maintain, for so long as Receiving Party has access to, creates, maintains, uses, or discloses [Agency's] Confidential Information adequate and appropriate safeguards in order to: (i) protect the confidentiality and security of Confidential Information obtained from, or created on behalf of, [Agency] by the Receiving Party, and (ii) prevent the use or disclosure of Confidential Information other than as provided for by this Agreement and applicable laws. Receiving Party administrative, physical, and technical safeguards and those of its subcontractors, shall comply with all applicable laws, and applicable then current privacy and security guidelines and/or standards issued by the National Institute for Standards and Technology (NIST). |

## Should include – Any other requirements imposed by law, regulation, contract or policy

*Include any other specific data sharing requirements that apply to the information. For example, HIPAA includes specific requirements for contracts with business associates accessing protected health information on behalf of a covered entity.*

## Might include – Term and termination

*Describe the effective term, which may end with a date or an event. Although not unique to data sharing agreements, including an appropriate term provision ties directly into data minimization and purpose limitation. Appropriate termination provisions tie directly into adequate enforcement remedies.*

**Examples**

| | |
|---|---|
| General term language | This DSA will begin on [beginning date] or date of execution, whichever is later, and continue through [ending date], unless terminated sooner as provided in this DSA. The DSA may be extended by mutual agreement through an amendment. |
| Termination for convenience | Either party may terminate this DSA with [# of days] days' written notice. Once Data is accessed by the Receiving Party, this DSA is binding as to the confidentiality, use and disposition of all Data received as a result of access, unless otherwise agreed in writing. |
| Termination for cause | [Agency] may terminate this DSA for default, in whole or in part, by written notice to the Receiving Party, if [Agency] has a reasonable basis to believe that the Receiving Party has:<br>(1) failed to perform under any provision of this DSA;<br>(2) violated any law, regulation, rule, or ordinance applicable to this DSA; and/or<br>(3) otherwise breached any provision or condition of this DSA.<br>If it is later determined that the Receiving Party was not in default, the termination shall be considered a termination for convenience. |



# Addendum A

## Might include – Off-shore prohibition

*Include a prohibition on storing or sharing information outside of the United States when prohibited by law, contract or policy. Even when not formally prohibited, before allowing information to be stored outside of the United States consider the ability to protect the information and seek recourse in a foreign jurisdiction. Also consider the criticality and sensitivity of the information, including the impact of the loss of confidentiality, integrity or availability.*

Examples

| | |
|---|---|
| General prohibition | Receiving Party must maintain all hardcopies containing Confidential Information in the United States.<br><br>Receiving Party may not directly or indirectly (including through Subcontractors) transport or maintain any Data, hardcopy or electronic, outside the United States unless it has advance written approval from [Agency]. |

## Might include – Cyber liability insurance

*Cyber liability insurance is a specific type of insurance coverage to protect an agency from the costs associated with a data breach or other cyber security issues. It is discrete from the commercial general liability requirements often included in agency contracts and the technology errors and omissions insurance that may be appropriate for contracts with IT vendors.*

*When sharing confidential information with outside vendors, agencies should require sufficient cyber liability coverage to protect the state in the event of a privacy or security incident. The appropriate amount many vary depending on the type and amount of information being shared, and the amount of information from other organizations covered by the policy.*

*State agencies may have their own cyber liability insurance purchased through the Department of Enterprise Services.*

## Might include – Indemnification

*This term serves to compensate an agency for harm or loss arising in connection with a vendor or contractor's actions or failure to act. The intent is to shift liability away from an agency on to the indemnifying party. Generally, this term should be included in all vendor and contractor agreements.*

**Examples**

| | |
|---|---|
| General indemnification | The Contractor shall be responsible for and shall indemnify, defend, and hold [Agency] harmless from any and all claims, costs, charges, penalties, demands, losses, liabilities, damages, judgments, or fines, of whatsoever kind of nature, arising out of or relating to a) the Contractor's or any Subcontractor's performance or failure to perform this Contract, or b) the acts or omissions of the Contractor or any Subcontractor.<br><br>b. The Contractor's duty to indemnify, defend, and hold [Agency] harmless from any and all claims, costs, charges, penalties, demands, losses, liabilities, damages, judgments, or fines shall include [Agency's] personnel-related costs, reasonable attorney's fees, court costs, and all related expenses.<br><br>c. The Contractor waives its immunity under Title 51 RCW to the extent it is required to indemnify, defend, and hold harmless the State and its agencies, officials, agents, or employees.<br><br>d. Nothing in this term shall be construed as a modification or limitation on the Contractor's obligation to procure insurance in accordance with this Contract or the scope of said insurance. |

## Might include – Third party requests

*Consider including processes for handling requests for information from third parties. This may include court orders and subpoenas or the Public Records Act, particularly when sharing information with other public agencies.*

**Examples**

| | |
|---|---|
| When sharing with other agencies | If the Receiving Party receives a public records request under Chapter 42.56 RCW for any records containing Data subject to this DSA, Receiving Party agrees to notify the [Agency] Public Disclosure Officer within five (5) business days and to follow the procedure set out in this section before disclosing any records.<br><br>The Receiving Party must provide a copy of the records with proposed redactions to [Agency] when they are available and ready. [Agency] will respond within ten (10) business days of receipt of the redacted records to identify concerns with disclosure of the records, propose any changes to the Receiving Party redactions, or request more time if needed. If Receiving Party disagrees with any of [Agency's] concerns or proposed changes, Receiving Party must notify [Agency] of that disagreement and provide [Agency] with a minimum of fifteen (15) business days to obtain a |

| | |
|---|---|
| | restraining order or injunction under RCW 42.56.540 before disclosing any records. |
| Acknowledgment of Public Records Act for bilateral sharing | Receiving Party acknowledges that [Agency] is subject to the Public Records Act (Chapter 42.56 RCW). This DSA will be a "public record" as defined in Chapter 42.56 RCW. Any documents or information submitted to [Agency] by Receiving Party may also be construed as "public records" and therefore subject to public disclosure. |

## Might include – Restrictions on disclosure or publication

*Some data recipients, such as researchers, may intend to publish data or analysis. Consider including publication procedures, such as de-identification standards or agency review prior to publication.*

### Examples

| | |
|---|---|
| General right to review publications | Any and all reports utilizing the data shall be subject to review by [Agency] prior to publication or presentation.<br><br>[If the recipient will publish analysis or reports using the data, consider the right to review. Also incorporate actual review process, including timelines for review] |
| Detailed right to review publications | All reports derived from Data shared under this DSA, produced by Receiving Party that are created with the intention of being published for or shared with external customers (Data Product(s)) must be sent to [Agency] for review of usability, data sensitivity, data accuracy, completeness, and consistency with [Agency] standards prior to disclosure. This review will be conducted and response of suggestions, concerns, or approval provided to Receiving Party within 10 business days. |
| Small numbers requirements | Receiving Party will adhere to [Agency small numbers guidelines] in any published reports. [Agency] and Receiving Party may agree to individual exceptions in writing (email acceptable). |

## Might include – Other widely applicable contract terms

*There are many generic contract terms (i.e. boilerplate) that may be appropriate for a DSA, that are not specific to the data sharing arrangement itself. Examples include governing law, severability, and order of precedence. These types of terms should be included when appropriate, and care should be exercised to ensure consistency when the DSA terms are used as an addendum or exhibit to another contract.*



# Addendum A

## Certification of Disposal of Confidential Information

| NAME OF RECEIVING PARTY: | CONTRACT #: |
|---|---|
| | |

_____ (Receiving Party) herby certifies that the data described below, received as a part of the data provided in accordance with the contract listed above have been disposed of.

You certify that you returned or securely destroyed all identified confidential information received from [Agency], or created, maintained, or received by you on behalf of [Agency]. You certify that you did not retain any copies of this confidential information.

Description of Information

_____
_____
_____
_____

Date of Destruction or Return: _____

Method(s) of disposal:

_____
_____

Disposed by:

_____

| Signature | | Date |
|---|---|---|
| Printed Name: | | |
| Title: | | |