ENTERPRISE information services

Privacy Guidance

for the handling and protection
of personal information by State of Oregon
Agencies, Boards and Commissions

02/13/26

DRAFT

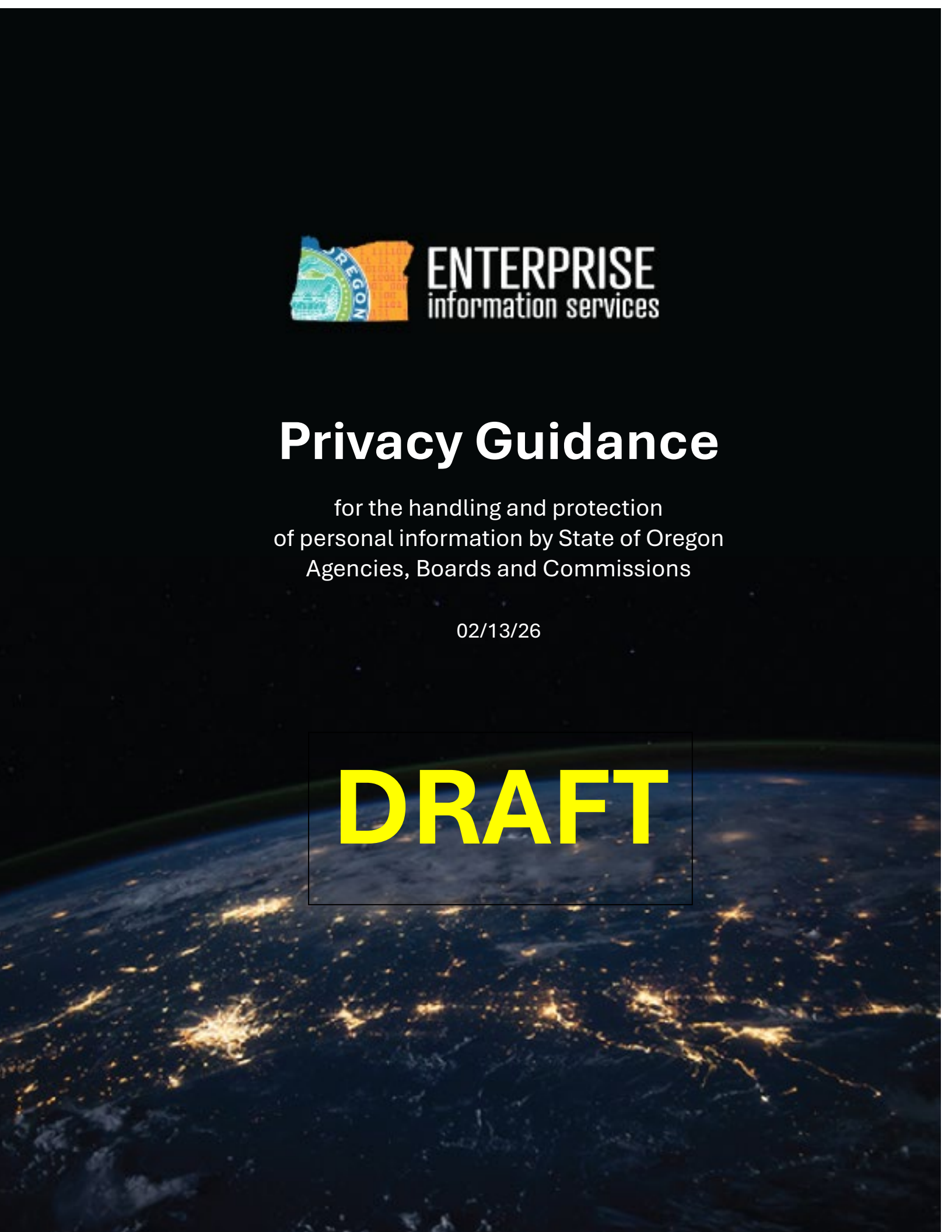

Table of Contents

Executive Summary

Purpose

The state of Oregon collects and uses personal information to deliver vital services, administer programs, and meet legal obligations. The purpose of this guidance is to support state agencies in their use and protection of Oregonian's personal information.

Overview

This document provides enterprise guidance for the handling of personal information by Executive Branch agencies. This includes the collection, use, sharing, storage, and disposal of personal information in any form when handled for state business purposes, including by administrative systems, analytics, automation, and artificial intelligence. This guidance is meant for all Executive Branch agencies, boards, and commissions under the purview of the State Chief Information Officer, as defined in ORS 276A.230, as well as any contractor, vendor, or other third-party processing personal information on behalf of those agencies.

This guidance:

- Describes the State of Oregon Enterprise Privacy Principles established by the Chief Privacy Officer, which are anchored in Fair Information Practice Principles (FIPPs)[1] and the National Institute of Standards and Technology (NIST) Privacy Framework[2] while maintaining Oregon's Information Asset Classification Policy[3] as the foundation for defining and applying privacy controls.
- Provides a list of recommendations for agencies on when to use and how to apply the principles, including a Privacy Review Checklist to use on new or existing processes, actions, or projects that involve the use of personal information.
- Includes a detailed Appendix with application examples for each privacy principle and a Privacy Controls matrix aligned to NIST, with recommended controls organized by data classification level.

Recommendations for Agencies, Boards and Commissions

The key recommendations for agencies are as follows:

1. Designate a Privacy Coordinator charged with integrating privacy considerations into data governance, project management, and procurement at the agency, and to serve as the primary liaison to EIS on privacy matters. This

[1] Fair Information Practice Principles (FIPPs) | FPC.gov
[2] Privacy Framework | NIST
[3] Information Asset Classification Policy 107-004-050.pdf

role could be part-time or combined with existing responsibilities and may not require creation of a new dedicated position or additional staffing.

2. Share the privacy review checklist with agency managers who oversee programs that handle personal information.
3. Encourage staff to use the privacy checklist when they have a new or changed use of personal information, including a new collection, a new use for existing data, or a new or changed data sharing agreement.

Ultimately, agencies are responsible for the data in their possession, and decisions on these recommendations rest with the agency. This guidance may be superseded by governing regulations for specific types of data held by agencies, including health data, criminal justice data, and educational data.

Definition of personal information

The term "personal information" is used throughout this document. As a baseline for the term, the Oregon Consumer Information Protection Act (ORS 646A.600) defines **personal information** as follows:

1. A consumer's first name or first initial and last name in combination with any one or more of the following data elements:
   - Social Security number;
   - Driver's license number or state identification card number issued by the Department of Transportation;
   - Passport number or other identification number issued by the United States;
   - Financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account;
   - Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction;
   - Health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or
   - Medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.

2. A user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification.
3. Any of the data elements or any combination of the data elements described in above if:
   - Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and
   - The data element or combination of data elements would enable a person to commit identity theft against a consumer.

The laws and rules for your agency may include additional elements of information that must be treated as personal information, and may use a different term. These laws and rules often have specific requirements for the information that you must follow.

Oregon Enterprise Privacy Principles

Enterprise Information Services (EIS) has developed these privacy principles to guide Oregon Executive Branch agencies in managing personal information responsibly. These principles are adapted from the widely accepted Fair Information Practice Principles (FIPPs) and aligned with the National Institute of Standards and Technology (NIST) Privacy Framework. These principles reflect agencies' legal obligations and operational realities, providing practical guidance for leadership and front-line staff alike. The goal is to help agencies build public trust by handling personal information lawfully, ethically, and transparently. Each principle below is explained in plain language, and a more detailed appendix connects each principle to FIPPs and NIST and includes examples.

1. Lawful, Fair, and Transparent Processing

Agencies should collect and use personal information in ways that are authorized by law, ethical and non-discriminatory, and transparent (open and clear to the public).

2. Purpose Specification and Use Limitation

Every collection of personal information should have a specific, explicit purpose, and personal information should not be used or shared beyond that purpose unless lawfully authorized.

3. Data Minimization and Collection Limitation

Agencies should collect the minimum amount of personal information necessary to accomplish their stated purpose, and no more.

4. Data Quality and Accuracy

Agencies should ensure that the data they maintain is accurate, complete, and up-to-date for the intended use.

5. Security Safeguards and Access Controls

Agencies should protect data with appropriate security measures and access controls per the Oregon Statewide Information Technology (IT) Control Standards.[4]

6. Individual Participation and Redress

Individuals whose data is collected should have the ability to access their data and correct inaccuracies, and if they believe their privacy has been violated they should have the ability to file a complaint.

7. Accountability and Governance

Accountability means there are defined roles, oversight, and the ability to demonstrate compliance, while governance is the internal framework (policies, procedures, and leadership support) that makes accountability real. This principle asks agencies to put in place the organizational structures and processes to manage privacy effectively

[4] eis-css-statewide-information-technology(IT)-control-standards.pdf

Agency Privacy Governance

Similar to the governance of information technology and data, agencies should incorporate privacy governance into their work. The recommended steps for doing so are as follows:

1. Designate an agency privacy coordinator. This individual should be charged with integrating privacy considerations into data governance, project management, and procurement at the agency, and to serve as the primary liaison to EIS on privacy matters. This role could be part-time or combined with existing responsibilities and does not necessarily require the creation of a new dedicated position or additional staffing.

2. Share this privacy guidance with agency leaders and managers who oversee personal information to help them understand when privacy risk should be considered and how to evaluate it, including understanding the four privacy risk evaluation triggers specified in the next section.

3. Have managers apply the Privacy Principles Checklist when appropriate. Identify areas of higher risk or uncertainty and complete the identified internal documentation and verification of external communication and processes.

Privacy Risk Evaluation Triggers

This process provides a recommended approach for agencies to consider privacy risks and mitigations when working with personal information. It is intended to support consistent, risk-based decision-making and to focus attention on changes that could materially increase privacy risk.

Agencies are encouraged to use the checklist when any of the following instances occur:

1. **New collection of personal information**: Any time an agency starts collecting personal information it did not previously collect, even if the program itself already exists.

   Example: A program adds a new intake form that now asks for date of birth, demographic data, or contact details that were not previously required.

2. **Making material changes to how personal information is used**: If there is a change in use or audience of already-collected personal information.

   Example: Data originally collected to administer a program is later reused for analytics, research, or performance reporting.

3. **Procuring systems that process personal information**: If the agency is buying, licensing, or substantially upgrading systems that handle personal information, regardless of whether the data is "new."

   Example: Procuring a case management, customer relationship management, human resources, or benefits system that stores or processes personal information.

4. **Making material changes to how personal information is shared**: If there is a change in a data sharing agreement which involves the use of personal information.

   Example: A new data sharing agreement is created, or an existing data sharing agreement is materially changed.

A good rule of thumb: If people would be reasonably surprised by the new or changed use of their information, use the checklist.

Privacy Review Checklist

This checklist provides recommendations designed to help agencies responsibly manage personal information, reduce risk, and align with statewide privacy principles. Not every checklist item will apply in all situations, so agencies should focus on the areas of highest risk and impact. Refer to the Appendix for further detail organized by information asset classification level.

Internal Documentation/ Practice	**Privacy Principle(s)**
☐ Identify and document the legal authority supporting each type of personal information collected. Collect only data elements reasonably necessary to achieve the stated purpose.	Lawful, Fair, and Transparent Processing Data Minimization and Collection Limitation
☐ Note the information asset classification level and whether regulated data is involved.	Lawful, Fair, and Transparent Processing
☐ Confirm that data uses are ethical, non-discriminatory, and aligned with public expectations.	Lawful, Fair, and Transparent Processing
☐ Periodically review data uses to prevent unintended expansion over time.	Purpose Specification and Use Limitation
☐ Follow existing retention schedules and secure disposal practices.	Data Minimization and Collection Limitation
☐ Use de-identified or aggregated data when possible.	Data Minimization and Collection Limitation
☐ Use authoritative data sources, when available.	Data Quality and Accuracy
☐ Maintain basic context such as timestamps or source information to support correct interpretation.	Data Quality and Accuracy
☐ Apply administrative, technical, and physical safeguards proportional to data sensitivity.	Security Safeguards and Access Controls
☐ Limit access by employees and third parties to personal information based on job responsibilities.	Security Safeguards and Access Controls
☐ Document internal roles and responsibilities related to personal information handling.	Accountability and Governance
☐ Retain basic records of privacy-related decisions and reviews.	Accountability and Governance

External Communication/ Confirmation	Privacy Principle
☐ Clearly disclose to the audience when information may be subject to public records laws and applicable exemptions.	Lawful, Fair, and Transparent Processing
☐ Clearly describe to the audience the purpose for personal information collection and intended use, including any sharing of their data.	Purpose Specification and Use Limitation
☐ Use reasonable validation controls at the point of collection.	Data Quality and Accuracy
☐ Provide a practical method for correcting known data errors that is appropriate to the program context, such as updating records through existing business processes, customer service channels, or internal review by the data or program owner.	Data Quality and Accuracy
☐ Make it reasonably clear how individuals can ask questions or raise concerns about their data.	Individual Participation and Redress

Appendix A: Privacy Principles Expanded Definitions and Examples

The following are more detailed definitions for each of the Oregon Enterprise Privacy Principles. Each section includes how the individual principle is tied to the FIPPs and NIST Privacy Framework, as well as specific examples. Also included are expanded recommendations and opportunities for agencies. Ultimately decisions on these recommendations rest with the agency. This guidance may be superseded by specific governing regulations related to the personal information.

1. Lawful, Fair, and Transparent Processing

What it means: Agencies should collect and use personal information in ways that are lawful (authorized by law), fair (ethical and non-discriminatory), and transparent (open and clear to the public). This principle aligns with FIPPs concepts of authority (ensuring legal basis) and transparency and supports NIST Privacy Framework functions Govern-P (establishing legal compliance) and Communicate-P (communicating data practices).

How to implement - To uphold lawful, fair, and transparent processing, agencies should:

- **Ensure legal authority:** Only collect or use personal information if you have statutory authority or a clearly defined business need that is permitted by law. Oregon agencies should identify the law, rule, or policy that authorizes each type of personal information they handle. For example, if an agency asks for a Social Security number, it should be because a law or program requirement necessitates it. If no authority exists, do not collect it. Document the legal basis (cite the Oregon Revised Statute(s) (ORS)/Oregon Administrative Rule(s) (OAR) or federal law) and include it in privacy notices or forms.
- **Provide clear notice:** Be transparent by informing individuals what information you collect, why you need it, how it will be used, and with whom it may be shared. Use plain-language privacy statements on forms, websites, or signage. Ensure the notice is easy to find and understand. For example, an agency's website privacy policy tells users that information they provide becomes a public record, outlines applicable laws, and explains what exceptions exist for personal privacy. Being upfront in this way allows the public to understand your data practices.
- **Practice fairness:** Use personal information in ways that people would reasonably expect and would not find deceptive or harmful. This means do not misuse data for purposes that would be considered unethical or that unfairly target or bias against certain individuals or groups. For example, do not collect data under false pretenses (no hidden surveillance or "secret" databases) and avoid discriminatory uses of data. Fairness also implies giving individuals appropriate respect and options – see Principle 6 on individual participation.

- **Be open about practices:** Agencies need to balance public records law with privacy. Most information collected by agencies is a public record, but Oregon law provides exemptions to protect individual privacy. Agencies should be candid with the public about what information could be subject to disclosure and what will be kept confidential. For example, if certain personal information (like home addresses) can be exempt from public disclosure due to privacy or safety concerns, explain that to individuals and honor those protections (under ORS 192.445 individuals can request nondisclosure of their home address in public records).

Example in practice*:* An agency that administers benefits programs ensures lawful, fair, and transparent processing by first confirming it has clear legal authority for every type of personal information it collects, such as citing the statute or policy that requires Social Security numbers for eligibility verification. The agency provides plain-language privacy notices on forms and websites explaining what data is collected, why it is needed, how it will be used, and with whom it may be shared. It avoids deceptive or discriminatory practices, ensuring that data is used only for purposes individuals would reasonably expect. The agency is also open about public records requirements and exemptions, informing individuals which information may be disclosed and what protections exist for sensitive details like home addresses. These steps build trust by showing that data practices are lawful, ethical, and transparent.

2. Purpose Specification and Use Limitation

What it means: Every collection of personal information should have a specific, explicit purpose, and personal information should not be used or shared beyond that purpose unless lawfully authorized. In other words, clearly state why you are gathering personal information, and then stick to that purpose when using the data. This principle comes directly from the FIPPs (Purpose Specification and Use Limitation) and is reinforced by the NIST Privacy Framework's emphasis on data processing policies. NIST advises organizations to establish policies that set conditions on data use and retention consistent with the original purpose. Agencies adopting this principle ensure that data isn't repurposed in ways that violate promises or surprise the public.

How to implement - To implement purpose specification and use limitations, agencies should:

- **Define and document the purpose:** For each type of personal information collected, explicitly document why it's needed and how it will be used. Do this through privacy impact assessments, form instructions, or internal data inventories. Make sure the purpose is legitimate and relevant to the agency's mission or service. For example, if an agency collects contact information for licensing, the purpose

might be “to contact license holders regarding renewals, recalls, or legal requirements.” Having this documented helps keep everyone on the same page.

- **Inform individuals of the purpose:** Include the purpose in the notice to individuals. Tell people upfront: “We are collecting X information to be used for Y purpose.” According to FIPPs, agencies should provide notice of the specific purpose for which personal information is collected. If possible, also inform them with whom the data may be shared for that purpose (e.g. “We will use your email to send you permit renewal notices and will not use it for other reasons without your consent or unless required by law”). Being specific builds trust and transparency.
- **Use data only for compatible purposes:** Once collected, do not use or disclose the data for any purpose that is incompatible with the original specified purpose. If a new use arises, you should ensure it is closely related to the original purpose or obtain additional authorization (either via law or consent). For instance, data collected for public health reasons should not suddenly be used for an unrelated research project or law enforcement inquiry unless a statute permits it or the individual consents. If an agency wants to repurpose data (say, using school children’s data for a new study), they should seek legal review and possibly get consent from the individuals or their guardians, because using it beyond the original intent could violate this principle and erode public trust.
- **Limit sharing to purpose needs:** Only share personal information with other agencies or third parties when it aligns with the original purpose or is required by law. If you do share data, establish agreements (MOUs or data sharing agreements) that restrict the recipient to using the personal data for the specified purpose. For example, if the Oregon Employment Department shares personal wage data with Oregon Housing Community Servies for a research project, the agreement should stipulate it’s solely for that project and cannot be used elsewhere. This ensures use limitation even after data leaves your agency. Any agreements that require legal sufficiency should be reviewed by the Oregon Department of Justice (DOJ).
- **Review and update purposes:** Over time, program objectives or legal mandates may change. Regularly review the purposes you have on file for collecting data. If they change, update your documentation and your public notices accordingly. Do not engage in “mission creep” silently – if you need to expand a use, do it transparently (update privacy policies, inform individuals, and if required, seek legislative authority).

Example in practice: An agency may collect personal information from individuals to fulfill a specific purpose, such as issuing licenses to ensure compliance and public safety. Under the principle of purpose limitation, that agency should not repurpose this data for unrelated activities, such as creating marketing lists for third parties. Legal frameworks, including federal and state privacy laws, typically enforce this principle by restricting the use of personal information to the original purpose (or closely related needs like audits or

archival requirements permitted by law). Agencies should follow this guidance: collect data for a defined reason and use it only for that reason.

3. Data Minimization and Collection Limitation

What it means: Agencies should collect the minimum amount of personal information necessary to accomplish their stated purpose, and no more. This is the principle of data minimization: do not ask for or retain personal information that isn't needed. It also implies limiting the scope of collection – in practice, do not collect overly detailed or intrusive data if a less-invasive option will suffice. FIPPs emphasize that personal information collection should be kept to a minimum. FIPPs additionally say to retain data only as long as necessary for that purpose. In the NIST Privacy Framework, this aligns with Control-P (data management practices) – for example, configuring systems to collect only what is required and to destroy data according to policy.

How to implement - Key practices for data minimization include:

- **Collect only what you need:** Review all forms, applications, and data systems to ensure each data element collected is directly relevant and necessary for the service or function. If something is nice-to-have but not essential, do not collect it. For example, if an online form asks for an applicant's Social Security number (SSN) but your process can work with just a name and case ID, remove the SSN field. Every piece of personal information collected is a potential risk (and burden), so be lean. Tip: During design of any data collection, ask "why do we need this item?" If there isn't a strong, lawful reason, don't include it.
- **Minimize at collection and use:** Not only limit the types of data, but also limit the amount collected. For instance, if asking for someone's date of birth to verify age, you might only need the month and year (or just year if that's sufficient) rather than full birth date. If you need location information, perhaps zip code will do instead of full address, depending on the purpose. By minimizing detail, you reduce sensitivity. Additionally, limit access to the data internally to only staff who are required to see it as part of their function, job, or role.
- **Use de-identified or aggregate data when possible:** If you can accomplish your goal with unidentifiable/de-identified or anonymized data, opt for that. For example, an agency evaluating program outcomes might use aggregated statistics instead of individual personal records. If analysis or testing can be done on fake or scrubbed data, use those instead of real PII. NIST's framework encourages measures to disassociate data from individuals when feasible. This reduces privacy impact while still enabling data-driven work.
- **Set retention limits and dispose of data:** Don't keep data longer than necessary. Follow Oregon's record retention schedules and dispose of data once the retention period or purpose is fulfilled, unless a law requires longer storage. Oregon's

Consumer Information Protection Act (ORS 646A.622) mandates that organizations securely dispose of personal information when it's no longer needed for business or required by law. This means shredding or permanently erasing records so they cannot be reconstructed. Agencies should have policies for purging databases or files of personal information after a certain timeframe. Regularly audit data stores and clean out expired personal information. By minimizing how long data lives, you minimize risk.

- **Periodically reevaluate data needs:** Over time, programs change. Perform periodic reviews of the data you collect to ensure it still meets a legitimate need. If you find you're collecting data that is not really being used or no longer necessary, stop collecting it. For example, if a survey once asked for participants' phone numbers but you never call them, consider dropping that field in future surveys. Continuous improvement in minimization will reduce the privacy footprint of your agency.

Example in practice: An agency running a public benefits program initially required a broad array of personal details on the application form. After applying the data minimization principle, the agency trims the form to only the essentials needed to determine eligibility (for instance, collecting income range instead of exact income). The agency also establishes that documents verifying eligibility will be destroyed after X years once they're no longer needed. These steps ensure the agency only holds what it truly needs to serve its purpose.

4. Data Quality and Accuracy

What it means: Agencies should ensure that the data they maintain is accurate, complete, and up-to-date for the intended use. This principle is about data quality – high-quality data leads to fair and effective decisions, while poor-quality (incorrect or outdated) data can harm individuals (for example, causing unjust denial of services or benefits). FIPPs refers to this as Quality and Integrity, meaning agencies should collect and use personal information with enough accuracy, relevance, timeliness, and completeness to ensure it is fair to the individual. In practice, this aligns with NIST's guidance that organizations should have processes for data review and correction (e.g., NIST's Control-P suggests enabling data to be altered or deleted to maintain quality). Simply put, decisions made with bad data are bad decisions – so agencies have a duty to keep data correct.

How to implement - To uphold data quality and accuracy, agencies should:

- **Verify data at collection:** Wherever practical, verify the information at the point of collection. This could mean using form validation (e.g., check that dates are in correct format, addresses exist, etc.), or cross-checking against known data. For instance, if someone registers a business and provides a ZIP code, ensure the ZIP

code matches the city given. If a citizen provides an ID number, check that it's the correct length/format. Simple validation reduces typos and errors that can propagate through systems.

- **Allow individuals to review and correct their data:** Individuals are often the best source for accuracy. Agencies should provide individuals with appropriate access to their personal information and an opportunity to correct or amend it. This could be through an online portal where people can update their contact information, or a process to submit corrections (such as, "If your information is wrong, call this number or fill out this correction form"). For example, Oregon's Public Records Law (ORS 192.355) exempts some personal information from disclosure partly to encourage individuals to engage with agencies without fear – but it also implies agencies should keep records accurate since they might be released. More directly, if a client notices their name or birthdate is recorded incorrectly in an agency's system, there should be a straightforward way to have that fixed. Accuracy is a shared responsibility between agencies and the individuals they serve.
- **Periodic data quality reviews:** Implement routine checks or audits of data accuracy. For important datasets, agencies can run audits (e.g., sampling records to check for common errors or outdated entries). If you have databases of addresses, consider using address validation services periodically to catch outdated addresses. If you maintain income or eligibility information, schedule periodic reverification. The goal is to catch errors or stale data proactively. NIST's framework encourages ongoing monitoring and review of privacy data to inform risk management – part of that is ensuring data remains accurate and fit for purpose.
- **Source data from authoritative systems:** Where possible, use authoritative sources to keep data accurate. For example, if one agency is the system of record for a certain data element (say, DMV for driver info or Oregon Health Authority for immunization records), other agencies relying on that data should synchronize or confirm with the source rather than maintain divergent copies. Integrations or data-sharing arrangements can help maintain consistency (with proper privacy safeguards). This way, each data point is updated at the source and propagated, reducing discrepancies. Always ensure such data sharing is lawful and transparent (tying back to Purpose and Minimization principles).
- **Maintain data integrity and context:** Accuracy isn't just about spelling of names or numbers – it's also about keeping data relevant and contextual. Make sure any context needed to interpret the data travels with it. For instance, if an agency logs that "Client X was sanctioned," it should also record the date and reason, so years later it's not misread out of context. Ensure that updates or corrections in one part of a record flow through to all relevant places in your systems. Keeping metadata (timestamps, sources) can aid in assessing data quality over time (e.g., knowing when the data was last confirmed).

Example in practice: An agency responsible for health programs maintains records to support service delivery and compliance. Applying the data quality principle, the agency implements measures such as verifying information against trusted sources, enabling individuals to review and correct their own records (as required by applicable laws), and periodically updating or archiving outdated data (e.g., removing inactive records or updating contact details through official change-of-address services). If an individual identifies an error, such as a missing entry, the agency provides a process to review and update the record upon valid documentation. These steps help ensure that decisions, like determining eligibility for services or issuing health alerts, are based on accurate information, promoting fairness and trust.

5. Security Safeguards and Access Controls

What it means: Agencies should protect data with appropriate security measures and access controls per the Oregon Statewide Information Technology (IT) Control Standards. This principle is about safeguarding confidentiality and integrity of personal information. No matter how lawfully or minimally you collect data, it won't matter if you can't keep it secure. Security Safeguards (a core FIPP) means implementing administrative, technical, and physical protections to prevent unauthorized access, use, alteration, or loss of personal information. This aligns with the NIST Privacy Framework's Protect-P function, which focuses on limiting the impact of security incidents through controls like access management, encryption, and regular maintenance. It also reflects Oregon law: the Oregon Consumer Information Protection Act (ORS 646A.622) requires any entity (including state agencies) that maintains personal information to develop and maintain reasonable security measures to protect that information and to prevent unauthorized access. In short, agencies have a legal and ethical duty to guard personal information as vigilantly as they would guard citizens' physical safety.

How to implement - Key security practices include:

- **Implement administrative safeguards:** Establish policies and procedures governing how staff handle personal information. This includes training employees on privacy and security awareness (e.g., how to recognize phishing, proper document handling) and defining roles and responsibilities for data protection. Limit which staff can access sensitive personal information – follow the principle of least privilege (only those who need access get it, and even then only to the data they need). Regularly remind and refresh training; Oregon Department of Human Services (ODHS)/OHA policy, for example, mandates security and privacy awareness training for all workforce members.
- **Apply appropriate technical safeguards:** Leverage technology to protect data. This includes access controls (unique user IDs, strong passwords, multi-factor

authentication, and role-based access so people only see what they should), encryption of data at rest and in transit (especially for sensitive data like Social Security numbers or health information), and network security measures (firewalls, intrusion detection systems, etc.). Follow the state of Oregon's Statewide Information Technology (IT) Control Standards (which align with NIST SP 800-53 controls) for information systems. Ensure that personal information stored on servers or cloud services is securely configured. For databases, implement audit logging to track who accesses or changes sensitive data (this not only deters misuse but also supports accountability). If you develop applications, build security in from the start – e.g., input validation to prevent injection attacks, proper authentication flows, etc.

- **Maintain physical security:** Don't overlook physical safeguards. Hard copy files containing personal information should be kept in locked cabinets or secure rooms with controlled access. The same goes for servers or storage media – keep servers in secure facilities with Data Center Services or other approved data centers with access badges, cameras, etc. For staff working remotely or in the field, provide lockable storage for documents and require safeguards for laptops (like cable locks in offices, never leaving devices unattended in cars, etc.). Ensure proper disposal of physical records – shred or pulverize papers containing personal information when they're no longer needed, as required by ORS 646A.622 for secure disposal.
- **Plan for incident response and breaches:** Despite best efforts, security incidents can happen. Per the Statewide Cyber and Information Security Incident Response policy, agencies are required to have an incident response plan specifically for data breaches involving personal information.
- **Continuously monitor and improve:** Security is an ongoing process. Utilize the Cyber Security Services resources – such as vulnerability scanning, risk assessments, and security audits – to identify weaknesses.

Example in practice*:* An agency that manages employment-related programs handles large volumes of sensitive personal information, such as names, addresses, Social Security numbers, and wage information. To comply with the security safeguards principle, the agency classifies this data as highly sensitive and enforces strict access controls, where only authorized personnel can view full identifiers, and they should authenticate using multi-factor login through secure systems. Databases are encrypted, and all access is logged and audited. Physical files are stored in secure facilities, and when retention periods expire, they are destroyed using certified shredding services. Staff receive annual privacy and security training, and the agency conducts regular vulnerability scans in partnership with its IT security team. In the event of a breach - whether through hacking or accidental exposure - the agency activates an incident response plan, notifies affected individuals, and provides assistance such as credit monitoring. These layered safeguards help protect personal information against unauthorized access, loss, or misuse.

6. Individual Participation and Redress

What it means: Individuals whose data is collected should have the ability to request access to their data and correct inaccuracies, and if they believe their privacy has been violated they should have the ability to file a grievance. This principle encompasses the FIPPs of Individual Participation and Access/Amendment. It means agencies should not treat personal information as one-way possession; rather, citizens have a stake in their own information. Individuals should be able to find out what data you have about them, influence how it's used (for instance, by consenting or objecting where appropriate), and have a channel to ask questions or complain. Redress refers to mechanisms for addressing complaints. If an individual believes their privacy has been violated or their data is incorrect, there should be a process to resolve that. NIST's Privacy Framework reinforces this by calling for processes to receive and respond to complaints and inquiries from individuals. Ultimately, this principle is about respecting the rights and dignity of the people we serve, by giving them voice and recourse regarding their personal information.

How to implement - Agencies can promote individual participation and redress through several practices:

- **Provide access to personal information:** Upon request, and as allowed by law or in accordance with Oregon Public Records law, individuals should be able to know what personal information you have about them. Many federal laws already grant this right (for example, individuals have a right to access their own records in systems covered by the federal Privacy Act; patients have rights under the Health Insurance Portability and Accountability Act (HIPAA) to see their health records). Even if not mandated by a specific law, it's a good practice. Oregon's Public Records Law gives any person the right to request records from public bodies, which would include their own data. In fact, Oregon Department of Justice's guidance confirms individuals have the right to review information collected about them. Agencies should establish a straightforward process for someone to request their data – this might be a form or contact point (e.g., "Contact us to request a copy of your information on file"). There can be exceptions (certain investigative or sensitive records might be restricted), but in general lean towards transparency with the individual about their own data.
- **Enable correction and amendment:** If an individual identifies that the information your agency holds about them is incorrect or outdated, have a process to correct it. This could mean updating your database, appending a note, or in some cases disputing and resolving records. According to FIPPs, agencies should provide an opportunity to correct or amend records to ensure accuracy. For example, if a

parent finds that their child's education record has a wrong address or a data entry error, the relevant agency should have a way to fix that record. Often, it's as simple as showing proof of the correct information. Make sure staff know how to handle such requests. Some agencies might have formal forms for record correction (as under the Family Educational Rights and Privacy Act (FERPA) for education records), but even without a mandated formality, treating the request seriously and updating your files is important. It not only improves data quality but shows respect for the individual. Note that for some agencies including law enforcement, under certain circumstances erroneous data may remain part of the individual's criminal history or police report.

- **Obtain consent when required or prudent:** In many government operations, consent is not the primary basis for data processing (authority by law is). However, there are cases where seeking the individual's consent or preference is appropriate. For example, if you want to use someone's personal testimony or photo in a publication, you'd get their consent. Or if an agency embarks on a new data sharing agreement that isn't clearly authorized by law, they might ask individuals to opt-in. Additionally, when collecting highly sensitive info for a new purpose, getting explicit consent is a way to ensure fairness. The Individual Participation FIPP suggests seeking consent for collection or use to the extent practicable. So, while you may not always be able to (or need to) get consent (e.g., you don't ask criminals for consent to collect their fingerprints – you have authority), when you do have a choice, involving the individual via consent or at least notification is good practice. Also consider providing privacy choices: for instance, an email subscription might let users decide how their email can be used (notifications only, or shared with partner programs, etc.). Giving people some control increases trust.
- **Establish a complaint and inquiry process:** Importantly, have a clear way for individuals to ask questions or voice concerns/complaints about privacy. Publicize this channel on your website or privacy notices ("If you have questions about how we use your data or if you believe your privacy rights have been violated, contact ___ at ___ or call ___"). When someone submits a privacy-related complaint – say they feel their information was improperly disclosed or they weren't treated fairly – the agency should have a procedure to investigate and respond. NIST's framework expects agencies to have processes for receiving, tracking, and responding to individuals' privacy concerns. Treat complaints seriously: acknowledge receipt, investigate what happened, fix any issues, and respond to the individual with the outcome or remedial steps. This not only resolves individual issues but can highlight systemic problems to fix. For example, if multiple people complain they weren't told their data would be shared with a third party, that signals you should improve your notice. Redress might also mean offering a remedy: e.g., if an agency mistakenly

exposes someone's personal information, an apology and mitigating assistance (like identity theft resources) might be appropriate.

- **Support individuals' rights under law:** Be aware of and prepared to uphold specific individual rights granted by laws. For instance, under Oregon law (ORS 192.445), a public employee or volunteer can request their home address/phone number be kept confidential if their safety is at risk – agencies need a process to mark records accordingly and refuse public disclosure of that info. Similarly, Oregon's new Consumer Privacy Act (2023 SB 619, effective 2024) gives Oregon consumers rights to access and delete certain personal information held by businesses (though it exempts state agencies, the ethos is relevant). Even if not strictly bound, agencies may voluntarily align with such best practices to the extent feasible. At minimum, ensure compliance with federal rights: e.g., the right to opt out of certain disclosures under FERPA for student records, or rights of individuals under the ADA or Civil Rights laws if data is used in decision-making (fairness rights).

Example in practice*:* An agency administering public assistance programs collects significant personal information to determine eligibility and deliver benefits. To uphold the individual participation principle, the agency provides systems for clients to access their case information, either online or through a caseworker. If a client notices incorrect data, such as income details that affect benefit levels, they can submit documentation to correct the record, and benefits are adjusted accordingly. The agency also maintains a complaint process: individuals who believe their information was mishandled or have a complaint can use an established feedback channel. Complaints are investigated, and if an error or breach occurs, the agency notifies the affected person and takes steps to mitigate harm, consistent with applicable laws. By enabling access, correction, and redress, the agency demonstrates accountability and respect for individuals' rights while meeting legal requirements.

7. Accountability and Governance

What it means: Agencies should be accountable for complying with these privacy principles and all applicable privacy requirements. Accountability means there are defined roles, oversight, and the ability to demonstrate compliance. Governance is the internal framework (policies, procedures, and leadership support) that makes accountability real. In practice, this principle requires agencies to put in place the organizational structures and processes to manage privacy effectively – from assigning responsibility, to training staff, to monitoring and auditing compliance. FIPPs includes Accountability as a principle: agencies should audit and document compliance, assign clear responsibilities to staff, and provide training. NIST's Privacy Framework similarly has a Govern-P function that involves establishing organizational privacy values, policies, and governance processes (including risk management, oversight, and accountability measures). Ultimately, privacy protection should be baked into the agency's governance just like financial stewardship or safety – it's

a management priority and a cultural value. Now, with enterprise efforts underway, agencies will need to coordinate with enterprise privacy governance too.

How to implement - Steps to foster accountability and governance include:

- **Assign privacy roles and responsibilities:** Agencies should designate who is responsible for privacy matters, an Agency Privacy Coordinator. This could be a Privacy Officer role (if resources allow, a dedicated person or team), or it could be an existing role such as the Agency Data Officer, Records Officer, or Information Security Officer taking on privacy duties. What's important is that someone at a sufficient level is charged with overseeing privacy compliance and championing these principles. Additionally, identify supporting roles: data stewards in various programs, IT leads for privacy, etc. Employees should know who to turn to with privacy questions (internally) and who is accountable. Oregon's state Data Governance Policy[5] already asks agencies to identify data stewards and assign responsibility for data management – privacy could be part of that remit. Clearly document these roles in org charts or charters. When roles are assigned, people can be held accountable for doing the job, and privacy doesn't fall through the cracks.
- **Develop and communicate internal policies:** Building on the enterprise principles, agencies should have their own internal privacy policies or procedures that translate these principles to the agency's specific context. For example, an agency might create a privacy policy manual or incorporate privacy rules into its employee handbook or administrative rules. Policies should cover how the agency handles personal information throughout its lifecycle (collection, use, sharing, retention, disposal), referencing these principles. Ensure the policies address compliance with any program-specific laws (i.e. if you deal with health info, incorporate HIPAA requirements; if you deal with education data, incorporate FERPA requirements). Once developed, communicate the policies to all staff through training, internal websites, and leadership messaging so everyone understands the expectations. Governance documentation sets the standard that staff are expected to follow.
- **Provide training and awareness:** Train your workforce on privacy responsibilities. Training should be role-appropriate. For example, front-line staff who collect data should be trained on providing notices and handling data properly, IT staff should be trained on privacy by design and data protection techniques, and leadership should be trained on oversight and risk management. Make privacy training a regular (e.g., annual) requirement, possibly integrated with security awareness training. New employees should receive privacy orientation as part of onboarding. Consider specialized training for high-risk areas (e.g., a caseworker dealing with sensitive

[5] Data Governance Policy 107-004-160.pdf

client info might get deeper training on confidentiality laws). Training and awareness programs ensure that the principles aren't just paper – they become part of daily practice. As FIPPs states, even contractors should be trained and aware of their privacy obligations if they handle state data.

- **Monitor, audit, and improve:** Build mechanisms to monitor compliance and continuously improve. This could include periodic privacy risk assessments or audits of how data is handled. For instance, an agency might do an annual self-assessment against these privacy principles (some states use checklists or privacy maturity assessments). Additionally, when things go wrong (like a breach or a significant complaint), treat it as a learning opportunity: investigate root causes, and update policies or training accordingly. NIST's framework expects organizations to review and update privacy practices as part of governance. Also, consider having an internal or external audit function periodically review privacy controls (similar to how financial audits occur). Accountability means being able to demonstrate to oversight bodies – and the public – that you are doing what you say you're doing. Keep documentation: maintain records of privacy notices issued, consent forms, training completion, privacy impact assessments, etc., as evidence of compliance.
- **Leadership and culture:** Finally, foster a culture of privacy through leadership tone. Agency leadership (directors, managers) should openly endorse the importance of protecting personal information and support initiatives to strengthen privacy practices. This might mean allocating budget for privacy measures (like tools or staff time for compliance tasks) and integrating privacy risk considerations into decision-making. For example, when launching a new program or IT system, leadership should ask "Have we addressed privacy risks? Did we do a privacy impact assessment? Are we following the enterprise privacy principles?" By making privacy a normal part of project approvals and strategic discussions, it becomes ingrained. Accountability isn't just top-down; encourage staff to speak up if they see potential privacy issues or have ideas to improve – create an environment where following these principles is recognized and rewarded, not seen as red tape. In essence, every employee should feel responsible for safeguarding personal information, and management should back them up with the proper framework and support.

Example in practice: An agency responsible for tax administration handles highly sensitive personal and financial data. To demonstrate accountability and governance, the agency designates a privacy leader (such as a Chief Privacy Officer) who oversees compliance and reports to senior leadership. It maintains detailed internal policies aligned with applicable laws and regulatory requirements, and all employees receive privacy training reinforced by clear consequences for mishandling data. The agency conducts regular audits to ensure records are accessed only for legitimate work purposes, with all access logged and monitored. Unauthorized browsing triggers alerts and corrective action. Leadership reviews privacy and security metrics as part of governance processes, and any breach or

error should be reported under relevant laws and regulations, creating strong incentives for robust oversight. This structured approach shows that roles are assigned, controls are implemented, and compliance is actively monitored. Agencies with less sensitive data should adopt a proportional level of governance to ensure privacy is managed effectively.

Appendix B: Detailed Privacy Controls

Purpose

The Privacy Controls Appendix provides a detailed matrix tying good privacy practices called for in the Privacy Review Checklist to the National Institute for Standards and Technology (NIST) Privacy Framework. If you have used the checklist and have questions on implementation, consult this section as well as the NIST Privacy Framework: NIST Privacy Framework Version v1.0.

Privacy Controls by Information Asset Classification Level

The Privacy Controls below presents privacy practices that agencies may consider to reduce privacy risk when working with personal information at different Information Asset Classification levels.

The matrix is not a checklist, mandate, or compliance standard. Agencies are not expected to implement every practice listed for a given classification level. Instead, agencies should select practices appropriate to their specific context, legal obligations, scale of data use, and potential impact on individuals, and document key decisions and tradeoffs.

Privacy Controls for Level 1: "Published" - Low-Sensitive Information

Information regularly made available to the public that, if disclosed, will not jeopardize privacy or security. Level 1 controls focus on transparency, appropriate use, and data quality rather than confidentiality or access restriction.

NIST Function	NIST Category	NIST Applicable Controls	Abbreviated NIST Implementation Guidance (consult NIST Privacy Framework for further details)
IDENTIFY-P	Inventory and Mapping (ID.IM-P)	ID.IM-P1, ID.IM-P4, ID.IM-P5	Maintain a basic list of systems and datasets that publish information publicly, including what data is released and for what purpose.
GOVERN-P	Governance Policies (GV.PO-P)	GV.PO-P1, GV.PO-P5	Follow enterprise privacy and public records policies when publishing information, including any legal requirements related to transparency and disclosure.
GOVERN-P	Awareness and Training (GV.AT-P)	GV.AT-P1	Ensure staff understand basic expectations for handling and publishing public information.
CONTROL-P	Data Processing Management (CT.DM-P)	CT.DM-P5, CT.DM-P6	Apply standard retention and disposal practices and use consistent formats when publishing or retiring public content.
COMMUNICATE-P	Data Processing Awareness (CM.AW-P)	CM.AW-P1, CM.AW-P3	Clearly communicate why data is published and how it is used, such as through website notices or contextual explanations.
PROTECT-P	Data Security (PR.DS-P)	PR.DS-P4, PR.DS-P6	Protect the availability and integrity of public information so it remains accurate and accessible.

Key Recommendations:

- Maintain inventory of published information systems
- Establish basic retention schedules
- Ensure public accessibility and availability
- Implement standard integrity checking

Privacy Controls for Level 2: "Limited" - Potentially Sensitive Information

Information that may not be protected from disclosure but could jeopardize privacy if made easily available.

NIST Function	NIST Category	NIST Applicable Controls	Abbreviated NIST Implementation Guidance (consult NIST Privacy Framework for further details)
IDENTIFY-P	Inventory and Mapping (ID.IM-P)	ID.IM-P1, ID.IM-P2, ID.IM-P3, ID.IM-P4, ID.IM-P5, ID.IM-P6, ID.IM-P7	Maintain a documented inventory that identifies data owners, types of individuals affected, key data elements, and where the data is processed or stored.
IDENTIFY-P	Risk Assessment (ID.RA-P)	ID.RA-P1, ID.RA-P3, ID.RA-P4	Consider how the data is used, shared, or accessed, and identify situations where misuse or exposure could reasonably create privacy concerns.
GOVERN-P	Governance Policies (GV.PO-P)	GV.PO-P1, GV.PO-P2, GV.PO-P3, GV.PO-P5, GV.PO-P6	Apply existing agency privacy and governance policies to internal or limited-access data, clearly defining roles and responsibilities.
GOVERN-P	Risk Management Strategy (GV.RM-P)	GV.RM-P1, GV.RM-P2	Use established agency processes to consider privacy risk and determine what level of protection is appropriate for the data.
GOVERN-P	Awareness and Training (GV.AT-P)	GV.AT-P1, GV.AT-P2, GV.AT-P3	Provide role-appropriate privacy awareness so staff understand expectations for handling non-public or internal data.
GOVERN-P	Monitoring and Review (GV.MT-P)	GV.MT-P1, GV.MT-P2, GV.MT-P3	Periodically review data uses, policies, and controls to ensure they remain appropriate as systems or business needs change.
CONTROL-P	Data Processing Policies (CT.PO-P)	CT.PO-P1, CT.PO-P2, CT.PO-P4	Establish clear internal rules for who may access, share, or modify the data, and align data handling practices with the system lifecycle.
CONTROL-P	Data Processing Management (CT.DM-P)	CT.DM-P1, CT.DM-P2, CT.DM-P3,	Define who can access or change the data, support routine updates/corrections, follow retention

		CT.DM-P4, CT.DM-P5, CT.DM-P6, CT.DM-P8	and disposal practices, and keep basic access logs where feasible.
COMMUNICATE-P	Communication Policies (CM.PO-P)	CM.PO-P1, CM.PO-P2	Establish how the agency communicates about data handling (internally or externally) and who is responsible for privacy-related communications.
COMMUNICATE-P	Data Processing Awareness (CM.AW-P)	CM.AW-P1, CM.AW-P2, CM.AW-P3, CM.AW-P4	Provide clear notices or explanations appropriate to the audience (for example, website notices or internal statements), offer a contact/feedback path, and keep basic records of disclosures when applicable.
PROTECT-P	Data Protection Policies (PR.PO-P)	PR.PO-P1, PR.PO-P2, PR.PO-P7, PR.PO-P9	Use standard IT practices like secure configuration, change control, and tested response/recovery procedures that cover systems processing this data.
PROTECT-P	Identity Management (PR.AC-P)	PR.AC-P1, PR.AC-P2, PR.AC-P4, PR.AC-P6	Use managed accounts, least-privilege access, and authentication appropriate to sensitivity (for example, MFA where warranted).
PROTECT-P	Data Security (PR.DS-P)	PR.DS-P1, PR.DS-P2, PR.DS-P3, PR.DS-P4, PR.DS-P5, PR.DS-P6	Protect data in storage and transit, maintain integrity and availability, and use reasonable safeguards to reduce accidental leakage or unauthorized exposure.

Key Recommendations:

- Follow agency data disclosure policies before external sharing
- Implement confidentiality/non-disclosure agreements for external/ third parties
- Maintain comprehensive data inventories
- Implement access controls and audit logging
- Conduct privacy awareness training
- Establish data retention and destruction procedures

Privacy Controls for Level 3: "Restricted" - Sensitive/Regulated Information

Sensitive information exempt from public disclosure. Includes personally identifiable information (PII) as defined in ORS 646A.602(12)(a)(A). Unauthorized disclosure could result in financial loss or identity theft. Level 3 practices emphasize risk reduction for sensitive or regulated data and are expected to be applied proportionally based on system scope, data use, and potential impact.

NIST Function	NIST Category	NIST Applicable Controls	Abbreviated NIST Implementation Guidance (consult NIST Privacy Framework for further details)
IDENTIFY-P	Inventory and Mapping (ID.IM-P)	**ALL** ID.IM-P1 through ID.IM-P8	Maintain a detailed inventory describing sensitive data elements, how they are used, where they flow, and which systems or partners are involved.
IDENTIFY-P	Business Environment (ID.BE-P)	ID.BE-P1, ID.BE-P2, ID.BE-P3	Clearly identify the system's purpose, role within the agency, and any priorities or constraints that affect how sensitive data is handled.
IDENTIFY-P	Risk Assessment (ID.RA-P)	**ALL** ID.RA-P1 through ID.RA-P5	Evaluate privacy risks associated with data use, sharing, or automation, and document key risks and mitigation approaches appropriate to the context.
IDENTIFY-P	Data Processing Ecosystem (ID.DE-P)	**ALL** ID.DE-P1 through ID.DE-P5	Understand and document third-party involvement, including contractual responsibilities and any privacy risks associated with external processing.
GOVERN-P	Governance Policies (GV.PO-P)	**ALL** GV.PO-P1 through GV.PO-P6	Apply agency privacy governance structures to sensitive data, including coordination with legal, procurement, and security functions where appropriate.
GOVERN-P	Risk Management Strategy (GV.RM-P)	**ALL** GV.RM-P1 through GV.RM-P3	Full risk management strategy considering data processing ecosystem role.
GOVERN-P	Awareness and Training (GV.AT-P)	**ALL** GV.AT-P1 through GV.AT-P4	Ensure personnel with access to sensitive data receive role-appropriate training, including expectations for handling regulated or high-impact information.

GOVERN-P	Monitoring and Review (GV.MT-P)	**ALL** GV.MT-P1 through GV.MT-P7	Periodically review data use, controls, and incidents or complaints to confirm safeguards remain appropriate as systems evolve.
CONTROL-P	Data Processing Policies (CT.PO-P)	**ALL** CT.PO-P1 through CT.PO-P4	Define internal rules for how sensitive data may be accessed, shared, or modified, including any applicable requirements related to individual rights.
CONTROL-P	Data Processing Management (CT.DM-P)	**ALL** CT.DM-P1 through CT.DM-P10	Apply enhanced data handling practices, such as access controls, logging, and minimization, particularly where automated or analytical processing is involved.
CONTROL-P	Disassociated Processing (CT.DP-P)	CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5	Use privacy-preserving techniques, such as de-identification or tokenization, where feasible to reduce exposure of sensitive data.
COMMUNICATE-P	Communication Policies (CM.PO-P)	**ALL** CM.PO-P1, CM.PO-P2	Establish clear processes for communicating about sensitive data practices, including roles and escalation paths.
COMMUNICATE-P	Data Processing Awareness (CM.AW-P)	**ALL** CM.AW-P1 through CM.AW-P8	Provide appropriate transparency and notification mechanisms, including processes for responding to incidents or individual inquiries.
PROTECT-P	Data Protection Policies (PR.PO-P)	**ALL** PR.PO-P1 through PR.PO-P10	Apply strengthened protection practices appropriate to sensitive or regulated data, including tested response and recovery procedures.
PROTECT-P	Identity Management (PR.AC-P)	**ALL** PR.AC-P1 through PR.AC-P6	Enforce strict access controls, least privilege, and authentication methods proportional to the sensitivity of the data.
PROTECT-P	Data Security (PR.DS-P)	**ALL** PR.DS-P1 through PR.DS-P8	Use comprehensive safeguards such as encryption, integrity controls, and environment separation to reduce the risk of unauthorized disclosure or misuse.
PROTECT-P	Maintenance (PR.MA-P)	PR.MA-P1, PR.MA-P2	Ensure system maintenance activities are authorized, logged, and performed securely.

PROTECT-P	Protective Technology (PR.PT-P)	**ALL** PR.PT-P1 through PR.PT-P4	Use protective technologies appropriate to the risk profile, such as network protections and monitoring capabilities.

Key Recommendations:

- Require contractual confidentiality obligations for external parties
- Implement rigorous confidentiality, integrity, and availability controls
- Conduct privacy impact assessments
- Implement de-identification and privacy-preserving techniques where appropriate
- Establish breach notification procedures that support both federal and state reporting obligations
- Maintain detailed audit logs
- Implement encryption for data at rest and in transit
- Conduct regular privacy risk assessments
- Establish incident response and business continuity plans
- Implement formal complaint handling processes.

Privacy Controls for Level 4: "Critical" - Extremely Sensitive Information

Information for named individuals only. Disclosure could cause major damage, injury, death, or significant harm.

NIST Function	NIST Category	NIST Applicable Controls	Abbreviated NIST Implementation Guidance (consult NIST Privacy Framework for further details)
IDENTIFY-P	**ALL Categories**	**ALL Subcategories**	Maintain the highest level of documentation for what data is processed, why it is processed, where it flows, and who is involved, especially for external partners or high-impact uses.
GOVERN-P	**ALL Categories**	**ALL Subcategories**	Use elevated oversight appropriate to risk, which may include senior leadership review for new or materially changed Level 4 processing, clear accountability, and role-based training for staff with access.
CONTROL-P	**ALL Categories**	**ALL Subcategories**	Apply the strictest handling practices appropriate to the situation, such as tightly limited access, strong authorization practices, and privacy-preserving techniques where feasible, particularly for analytics or automation.
COMMUNICATE-P	**ALL Categories**	**ALL Subcategories**	Establish clear escalation and communication procedures for incidents and high-impact events, including timely notification practices consistent with law, policy, and incident response processes.
PROTECT-P	**ALL Categories**	**ALL Subcategories**	Apply maximum protection appropriate to risk, which may include strong encryption, enhanced monitoring, and additional technical safeguards for systems processing Level 4 data.

Note: Entries in this matrix describe examples of practices that may help reduce privacy risk. They are not exhaustive or mandatory.

Appendix C: Definitions and Regulated Data Categories

Access controls: Mechanisms for granting or denying requests to use information or systems. (NIST Glossary)

Aggregated data: Summarizing information; often used to mitigate privacy concerns. (Open Data Standard Guidance)

Data classification level: Categorization of information assets into Levels 1–4 based on sensitivity and harm if compromised. (Statewide Information Asset Classification Policy)

Data Minimization: Limit collection to personal information that is adequate, relevant, and reasonably necessary for specified purposes. (ORS 646A.578)

Data Quality: Dataset quality based on standards adherence, metadata completeness, accuracy, and open format. (Open Data Standard Guidance)

De-identified Data: Data that cannot reasonably be linked to an identifiable consumer/device. (ORS 646A.570)

Encryption: An algorithmic process that renders data unreadable or unusable without the use of a confidential process or key. (ORS 646A.602)

High-Value Data: Data that improves accountability, public knowledge, mission delivery, economic opportunity, or meets public demand. (Open Data Standard Guidance)

Machine-Readable: Data that can be easily processed by a computer without losing any semantic meaning. (Open Data Standard Guidance)

Metadata: Data about data; describes characteristics such as title, description, keywords. (Open Data Standard Guidance)

Multi-Factor Authentication: Authentication requiring two or more distinct factors. (NIST Glossary)

Personally Identifiable Information (PII): Information that can be used alone or with other data to identify an individual. (Oregon's Open Data Standards)

Privacy Impact Assessment (PIA): Formal analysis/document to evaluate privacy risks and mitigations. (NIST Glossary)

Publishable Data: Agency data except categories restricted by law, privacy, deliberative process, proprietary protections, security, employment records. (Open Data Standard Guidance)

Retention Schedule: Official schedule specifying how long records must be kept and final disposition (retain/destroy/archive).

Role-Based Access Controls (RBAC): Access control based on roles with assigned permissions. (NIST Glossary)

Regulated Data

Regulated data is subject to sector laws requiring additional safeguards, including the following:

Criminal Justice Information Services (CJIS): Covers Criminal Justice Information (CJI) such as criminal history records, biometrics, warrants, and investigative law enforcement data; governed by the FBI CJIS Security Policy with strict access control, auditing, encryption, and personnel requirements.

Family Educational Rights and Privacy Act (FERPA): Protects student education records and personally identifiable student information; applies to K–12, higher education, and agencies receiving student-level education data.

Federal Tax Information (FTI): Federal tax return and taxpayer data received from the IRS; governed by IRC §6103 and IRS Publication 1075 with some of the strictest safeguarding and audit requirements in government.

Health Insurance Portability and Accountability Act (HIPAA): Protects individually identifiable health information (PHI); applies only where the agency is a Covered Entity (e.g., OHA) or Business Associate.

Appendix D: Additional Resources

2023 Statewide Information Security Program Plan
Oregon Enterprise Information Services
https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-statewide-information-security-program-plan.pdf

Fair Information Practice Principles (FIPPs)
Federal Privacy Council
https://www.fpc.gov/resources/fipps/

NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0
National Institute of Standards and Technology (NIST)
https://doi.org/10.6028/NIST.CSWP.01162020

Oregon Identity Theft Protection Act (ORS 646A.600-628)
Oregon Legislature
https://oregon.public.law/statutes/ors_646a.622
https://www.oregonlegislature.gov/bills_laws/ors/ors646a.html

Oregon's Open Data Standard
Oregon Enterprise Information Services
https://data.oregon.gov/Administrative/Oregon-s-Open-Data-Standard/ewk6-d856/about_data

Records Retention Schedules
Oregon Secretary of State
https://sos.oregon.gov/archives/Pages/records_retention_schedule.aspx