With privacy being a major concern among the public and a top risk for both private and government entities, University Compliance Services distributes the Privacy Matters @ WWU newsletter to highlight important privacy developments and to provide a centralized platform where University Privacy Owners and stakeholders can connect on privacy topics in an effort to strengthen Western’s Privacy Program.

In this Newsletter

- What is the Difference between Data Privacy and Information Security?
- State Privacy Policy Update
- State Grant Opportunity for Data Privacy and Security Projects

What is the difference between Data Privacy and Information Security?

Information security and data privacy are two business strategies that people often mistakenly use interchangeably. While they are not the same, they do overlap, sharing common goals and risks.
Data privacy deals with what, how, and why personal data is collected, used, and shared while information security is concerned about whether the processes and systems by which the data is collected, accessed, stored, and disposed of are secure.

Data privacy also focuses on being transparent and compliant in terms of honoring individuals' right to reasonably control the collection, use, disclosure, and disposal of their data. For example, certain laws require obtaining an individual's written consent before sharing their personal data and some laws require entities to inform individuals before collecting their data about how it will be used and shared enabling them to make an informed decision about whether to provide the data at all or to limit what they provide.

Information security protects an organization's physical and electronic data, both personal and non-personal, by implementing controls to prevent unauthorized access to data, systems, and networks. Data privacy is also focused on protecting data from unauthorized access, use and disclosure but is only concerned about personal data in any format (e.g., hard copy, electronic, verbal, images, audio).

How Data Privacy and Information Security Overlap

1. Both share the goal of protecting confidential data from unauthorized access, use, and disclosure.

2. Both require implementing internal controls throughout the data lifecycle from the point of collection to the point of destruction.

3. Both subject the University to reputational, operational, and financial harm if sufficient and effective controls are not implemented.

4. Both face the challenges of ever-changing regulations, consumer expectations, systems and processes, and increased collection of data.

It's possible to meet security requirements without considering privacy. However, without adequate security, nothing is private. Prioritizing the protection of personal data both from a privacy and security perspective will foster trust among Western's constituents and support its efforts in maintaining legal compliance, financial stability, and a sustainable reputation.

State Privacy Policy Update

Compliance Services is monitoring the development of two policies expected to be published this June by WaTech.

Privacy and Data Protection Policy

The proposed requirements of this policy include, but are not limited to, state agencies must:

1. Understand the personal information that the agency processes via various documented activities.
2. Conduct Privacy Impact Assessments and ensure data sharing agreements are in place with third parties when personal data is involved.

3. Implement employee privacy awareness training.

4. Dispose of confidential data when it has met its record retention requirements.

5. Be transparent about how personal information is processed by publishing privacy notices.

6. Allow individuals to reasonably access or correct their information maintained by the agency.

7. Implement controls to identify, report, and respond to privacy incidents and reviewing data handling practices.

**Access Control Policy**

The proposed requirements of this policy include, but are not limited to:

1. Managing user or system access throughout the account life cycle (from the identification of a user to the granting, modification, or revocation of a user’s access privileges).

2. Granting access using the least privilege principle.

3. Separating conflicting access privileges such that no one person is able to perform any tasks that lead to fraudulent activity.

4. Determining access levels of a user in the system based on the user’s role.

---

**State Grant Opportunity for Data Privacy and Security Projects**

WaTech announced that the next State and Local Cybersecurity Grant Program application is available for privacy or security projects to be funded. Cybersecurity or privacy projects that align with the objectives of the grant program and state cybersecurity plan will be considered.

The **deadline for applications is May 10, 2024.** Go to the [State & Local Cybersecurity Grant Program | WaTech](https://www.wa.gov/wat) for more details.

Last year funds were approved to provide a limited number of vouchers for privacy professionals at various Washington state agencies to receive privacy training and certification through the International Association of Privacy Professionals (IAPP). Nicole Goodman was one of the voucher recipients and is currently completing the national privacy certification training.

Please send in your newsletter content comments, suggestions, and questions to [compliance.matters@wwu.edu](mailto:compliance.matters@wwu.edu)