Written by: Novak, Sam (3/9/2023 11:58:00AM)

Updated by: Novak, Sam (3/9/2023 11:58:00AM)

Approved by: Zuge, Peter (6/21/2023)

UWSP Information Security Program

Mission statement

The mission of the UWSP Information Security Office is to safeguard the confidentiality, integrity, and availability of information systems, identity, and data assets by providing proactive security expertise, creating, and maintaining a resilient and secure infrastructure, and fostering a culture of security awareness and compliance throughout the organization. The UWSP Information Security program (ISP) is overseen and implemented by the UWSP Information Security Office (ISO), a unit of UWSP Information Technology (IT). ISP is led by the Chief Information Security Officer (CISO) at the behest of the Chief Information Officer (CIO) as a function of Academic Affairs. The CISO is responsible for ensuring that information is adequately protected within our and our affiliates information systems while also supporting the needs of the University.

This program is in addition to and in alignment with the University of Wisconsin System Information Security Policy.

Program Design

The design and direction of the ISP is driven by:

- United States Federal Law
    - Laws and Acts such as FERPA, HIPAA and GLBA (Gramm Leach Bliley Act) have requirements that drive certain objectives of the ISP.
- UW System administrative policy
    - SYS 1000 Series: Information Security
    - As a member institution of UW System, we are bound to comply with UW System policy.
- University business objectives
    - One of the goals of Information Security is to support the direction of the business, and help it achieve its business objectives.
- Regularly preformed risk assessments and audits
    - Based on the findings of risk assessments and regular audits, ISP will develop and implement security controls to manage risks before they become incidents.
- Industry trends
    - Information technology, being an ever-evolving field, will spur changes to move to a more secure future, and the ISP remains ever vigilant in looking for new ways to further enhance the security of our users and their information.

Information security program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Program Details

- Risk Assessments
    - Risk assessments aim to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could results in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.
    - Risk assessments include:
        - Criteria for the evaluation and categorization of identified security risks and threats faced by the University.
        - Criteria for the assessment of the confidentiality, integrity and availability of our information systems and customer information, including the adequacy of the existing controls in the contact of the identified risks or threats faced by the University.
        - Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the ISP will address the risks.
    - Risk assessments will regularly be reviewed to ensure the efficacy of the controls put in place, and to review if additional risks need to be considered.

- Safeguards and Security Controls
    - Based on the results of risk assessments, the ISO will develop safeguards and security controls, such as authentication, segmentation, or isolation, to ensure the confidentiality, integrity and availability of the information and systems being assessed.
    - Safeguards and Security Controls include:
        - Access control
            - Access controls, both technical and, if appropriate, physical, are utilized to authenticate and permit access to authorized users, while protecting against the unauthorized acquisition of customer information. Access controls are additionally utilized to limit authorized users' access only to customer information that they need to perform their duties and functions, or in the case of customers, to access their own information.
        - System Management
            - IT utilizes several different endpoint management systems (EMS) to ensure that our endpoints are uniformly configured for optimal functionality and security, based on the types of information being processed by that system.
        - Encryption
            - Encryption is used by IT to ensure that information is protected in transit within UWSP information systems, and encrypted at rest when the information being handled is considered sensitive in nature.
        - Software development
        - Multifactor Authentication

        - IT utilizes multifactor authentication to protect all external authentication attempts coming into university systems, and to protect our cloud assets.
    - Data Retention
        - IT retains records for the length prescribed by law and disposes of them in accordance with their sensitivity.
    - Change Management
    - Monitoring and Logging
        - IT implements extensive log recording, collecting information from many components of our IT infrastructure.

Access to information

- Access to information is controlled with role-based access controls, ensuring that only those that are authorized to access pieces of information can do so. Privileged roles are monitored for change to further prevent unauthorized access.

Collection of information

- Information may be collected via forms, cookies, or other automated functions. A privacy policy for the specific service may better detail the methods of collection.

Distribution of information

- Information is not shared with third parties without notice, unless required to disclose information to law enforcement or other entities with a legal authority to obtain said information. Details about which third parties information is shared will be outlined in the privacy policy for a specific service.

Processing of information

- Obtained information is processed by the system that obtains it unless additional external processing is needed to complete the processing objective.

Protection of information

- Information is protected in a manner appropriate for its sensitivity using encryption, access controls and extensive auditing for record keeping purposes.

Storage of information

- Information is stored in a manner appropriate for its sensitivity using encryption, physical access controls and technical controls to prevent unauthorized access.

Usage of information

- Information collected as part of a process or over a service will be used by the system collecting it and any external entities outlined in the privacy policy for a specific service.

Disposal of information

- Information disposal is a vital component of the information lifecycle. To prevent unauthorized access to information stored on workstations, all devices as encrypted to the highest possible degree without affecting functionality. Devices that are not encrypted are wiped in a manner appropriate for the highest sensitive of information stored on the device before resale. If a device is not possible to securely wipe, it is recycled by an authorized third party. Server storage is sent to an authorized recycler for shredding after it has exited service.

Definitions:

Information Systems:

Information system means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.

16 CFR 314.2(j)

https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.2(j)