Document version: 1.00
Approval date: 5/9/2024
Approved by: Peter Zuge (CIO)

UW Stevens Point Information Security Incident Response Policy

Purpose

Cybersecurity attacks continue to evolve in both sophistication and frequency. Accidental disclosure of information can also occur. Having a well-tested plan to respond to information security incidents is needed so that any incident can be dealt with in a timely manner, reducing the exposure and risk to the data and Institution.

Scope

The scope of this policy is limited to information security incidents. This policy applies to all individuals who have access to protected University of Wisconsin-Stevens Point (UW Stevens Point) information and resources and provides the minimum requirements for information security incident response.

Definitions

Information Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Examples include, but are not limited to, unauthorized data access, accidental disclosure or exposure of sensitive information, an active denial of service attack, or a threat from a widespread malware attack in which systems are vulnerable.

Protected data: Any UW Stevens Point data and resources assigned a classification level other than public, as defined in the Universities of Wisconsin System Administrative Policy 1031: Information Security: Data Classification (Universities of Wisconsin System, 2024).[1]

[1] Universities of Wisconsin System. (2024, May 1). *Information Security: Data Classification*. Retrieved from UW Policies: https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification

Policy Statement

Any individual who suspects that an information security incident has likely occurred, must report it to the appropriate institution personnel.

All suspected information security incidents will be tracked.

Personnel involved in Information Security incidents must cooperate with investigation teams and provide access to institution owned assets.

Where personally owned assets are involved, cooperation is required to ensure no institutional data is at risk or has been compromised.

The UW Stevens Point Information Security Incident Response Plan will be used to further define the requirements for Information Security incident response.

The Chancellor and the CIO will review the IS incident events on a quarterly basis.

Per UW System Administrative Policy 1033 – Information Security: Incident Response, last revised on August 23, 2022, UW Stevens Point will communicate with UW System Administration as follows:

- Written initial notification is provided to the Office of Information Security (informationsecurity@uwsa.edu) within one business day of discovery
- Follow-up written notification is provided to the Office of Information Security within three business days of discovery
- A final findings report and the incident closure date are provided to the Office of Information Security
- The Traffic Light Protocol (TLP) is used during all written communications
- Refer to UW System Administrative Policy 1033 for the most up-to-date information

Related Documents

- UW System Administrative Policy 1031 – Information Security: Data Classification and Protection
- UW System Administrative Policy 1031.A – Information Security: Data Classification
- UW System Administrative Policy 1033 – Information Security: Incident Response
- Cybersecurity & Infrastructure Security Agency – Traffic Light Protocol

Scheduled Review

This document will be reviewed on an annual basis, or as deemed necessary.

Revision/Review Log

Date	Approver	Action	Description
		New policy	Created based on the requirements contained in the May 1st, 2024 version of the University of Wisconsin System Administrative Policy 1033 - Information Security: Incident Response.

References

Universities of Wisconsin System. (2024, May 1). *Information Security: Data Classification*. Retrieved from UW Policies: https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification