This message is being sent to Provosts, CBOs, SSAOs, CDOs, CIOs, Technology and Information Security Council, and Identified Campus Representatives.

UW SYSTEM ADMINISTRATIVE POLICIES

Information Security Policies and Procedures Approved


Please see a detailed description of the new policies and procedures below.

SYS 1000, Information Security: General Terms and Definitions

This policy will be effective upon approval.

Summary of Policy and Policy Revisions

- The purpose of this policy is to provide a list of general terms and definitions that are used in the 1000 series of the UW System Administrative policy set as well as additional definitions, as required, to provide clarity and consistency across all UW System Administration information security policies, documents and systemwide initiatives.

- New definitions, and material edits to existing definitions, will be circulated for institutional vetting prior to addition to this policy.
Affected Areas on Campuses

- This policy applies to all institutions and areas on campus when interpreting the 1000 series of UW System Administrative policies.

Expectation of Campuses on UWSA Policy Reporting

- No reporting or implementation steps are required by institutions.

Additional Communication

- No additional communications are anticipated at this time.

SYS 1039, Information Security: Risk Management

This policy and these procedures will go into effect on April 1, 2021.

Summary of Policy and Procedures

This policy and procedures have been developed to establish expectations for Information Security Risk Management activities, as described below.

SYS 1039: The policy provides a formal structure for the management of information security (IS) risks occurring within the University of Wisconsin (UW) System.

SYS 1039.A: This procedure establishes the process for the management of information security risks faced by the institutions of the University of Wisconsin (UW) System.

SYS 1039.B: This procedure defines the specific method and information required to document, track and provide notification of risk acceptance of information security-related requirements throughout the University of Wisconsin (UW) System.

These three documents establish the foundation for a UW-Systemwide Information Security Risk Management Program. The policy and associated procedures address core pillars of information security risk management, setting associated expectations for UW faculty and staff.

The policy has been developed to ensure UW's compliance with current and future information security governance, risk and compliance needs. Key components of this policy and procedures include:

SYS 1039, Information Security: Risk Management

- Establishes standard methods for Information security risk management associated with all institution owned or leased information systems that process, maintain, transmit or store data used to accomplish UW System research, teaching and learning, or administration.

- Establishes standard methods to ensure that the likelihood and impact of threats and vulnerabilities are understood and minimized to the furthest extent practical.
• Creates a repository known as the Risk Register, for the identification, management, reporting, and tracking of implementation of controls, in relation to Information security risks and the assessment of those risks.

• Documents accepted risks in situations in which a UW institution does not implement a standard control or process.

• Establishes responsibility for ensuring information security risk management training materials are made available to leaders, managers, system developers and users.


• Establishes the process for the management of information security risks faced by the institutions of the University of Wisconsin.

• Enables UW System institutions to proactively assess, mitigate, and manage information security risk throughout the enterprise.

• Enables UW System institutions to capture information security risks in a formal, standardized manner.

• Assigns formal information security risk ownership, treatment and validation.

• Establishes a formal method for the assessment of likelihood, impact and resulting overall information security risk(s) throughout UW System.


• Defines the specific method and information required to document, track and provide notification of risk acceptance of information security-related requirements throughout the University of Wisconsin (UW) System.

Affected Areas on Campuses

• Each institution's information technology office, led by its Chief Information Officer (CIO), is responsible for communicating this policy and associated procedures to its community of constituents.

• This policy and associated procedure documents are applicable to all institutions, schools, departments and employees of UW System, including academic staff, university staff, faculty, student employees, and researchers, as well as third-parties, such as authorized contractors and vendors, who have access to UW System data and/or systems.

Expectation of Campuses on UWSA Policy Reporting

• It is expected that the identified institution's Chancellor or their designee will regularly report to UWSA on the implementation status of this policy and the associated procedures.
Additional Communication

- The UW System Office of Information Security will ensure information security risk management training materials are made available to UW System leaders, managers, system developers and users.

- Further reminder communications will be sent prior to the effective date.

Stay updated with the policy development process by subscribing to an RSS feed [here](#). You can use this feed with your favorite RSS reader or subscription service.