UW-Madison

Cybersecurity Risk Management Policy

April 18, 2017 version

as endorsed by the Information Technology Committee on May 19, 2017

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

SUMMARY

Cybersecurity is a collective responsibility which requires policy that applies to all components of the University of Wisconsin-Madison. The impact of using diverse but competing approaches in implementing security controls applied to information systems tends to elevate overall cybersecurity risk[1]. The management of cybersecurity risk will use a detailed framework to balance among academic / business needs, the potential impact of adverse events, and the cost to reduce the likelihood and severity of those events.

This policy and the associated Risk Management Framework applies to all university information systems and provides a common approach to managing risk to university data and the information systems which process, store or manage the data.

POLICY

Cybersecurity risk will be managed to ensure likelihood and impact of threats and vulnerabilities are minimized to the extent practical. Guided by the Principles below, the focus of this policy is protection of University information or data and the associated information system or computing assets, which includes those systems developed or purchased for integration with the existing information technology architecture. Information and data sets not owned by the University may become within scope of this policy if the data will be stored or processed using University assets.

The Cybersecurity Risk Management Process, described in the Implementation Procedures of this policy, is the mandatory process for managing the cybersecurity risk associated with all information systems of any kind that store or process data used to accomplish UW-Madison instruction, research, public service, or administration.

The process will be phased in. High risk systems will be first, with moderate and low risk systems to follow. The activity level to secure a system will be proportional to the data driven categorization of the information system and intended level of risk with the system in operation.

The Office of Cybersecurity will provide mandatory cybersecurity training for leaders, managers, and users. Training will be appropriate to the audience, and will be phased in over time.

PRINCIPLES

The University of Wisconsin-Madison is a leading public institution of learning and higher education. As such, our mission is to create and disseminate knowledge and to learn the truth wherever it may be found. Fundamental to this mission is the academic freedom, the "fearless

[1] From *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute for Standards and Technology, February 2014

sifting and winnowing" process emblazoned at the entrance to Bascom Hall by the class of 1910.

Recognizing that the level of monitoring and analysis employed for network defense against cybersecurity threats by using this Risk Management Framework can have a significant chilling effect on learning and academic freedom, the Office of Cybersecurity will operate under the following principles guiding the deployment and use of this framework:

1. We respect academic freedom and personal privacy as we provide a secure and safe computing environment for teaching, research and outreach as well as to protect the integrity and reputation of UW-Madison.
2. We understand the value of University information as a product of research, data related to teaching and learning, along with the personal data of our students, faculty, researchers, and administrative staff.
3. We are committed to ensuring the appropriate security of all data, specifically ensuring students privacy and security of staff related information is not placed at undue risk of exposure.
4. We are accountable to the University community for our deployment and use of network analysis and monitoring tools. Our activity preserves and strengthens the privacy and academic freedom for faculty, students, staff, and members of our community.
5. We will ensure risk analysis tools and active filtering methods will be used only for the detection of malicious activity, not for examining any other content in the data stream.
6. We evaluate the content of systems and network traffic only to the extent necessary to detect known security threats or emerging indications of compromised systems. Specifically:
    a. Our tools and techniques are not used to monitor individual activity. Data generated or collected that may identify individual behavior will be retained no longer than is necessary to identify and evaluate malicious traffic.
    b. Data generated by the framework and tools is used only to detect threats and compromises. Any personal or private message content captured during the testing and detection processes is ignored, and either not recorded at all, or eliminated immediately in cases where temporary recording is necessary technologically.
    c. Data collected is accessible only by staff responsible for maintaining the security of computing systems, and only for the purpose of diagnosing and remediating security incidents. This data will not be released for any other purpose, except as may be required to comply with legal requests.
7. We make decisions on network and cybersecurity defensive measures through a defined and shared process that implements the principles above. We will ensure that our processes:
    a. Allow for temporary situations where immediate defensive action is needed.
    b. Review those temporary measures through the decision-making process, to determine if they should become ongoing.
8. The procedures that implement the RMF processes are developed with collaboration in mind and will be revised collaboratively as conditions warrant.

BACKGROUND

The risk management process is established in policy so that the UW-Madison community can share a common understanding that:

1. UW-Madison is determined to manage cybersecurity risk effectively. Not doing so is likely to have unacceptable consequences to individuals and increase cost to the institution.
2. This is UW-Madison's mandatory and universally applicable process for managing cybersecurity risk.
3. This process can be tailored to specific technologies, processes or services. This policy applies to UW-Madison owned or operated information systems and architectures that are installed on campus or accessible through external services (e.g., cloud infrastructure, services or applications, vendor-operated systems using University information, systems operated remotely from other universities, etc.).
4. The process must include policy and procedural controls to assure that privacy and academic freedom are respected.

A separate Implementation Plan is being refined and will accompany the Policy and with detail training, timelines, and processes.

AUTHORITY

TBD [will depend upon who issues the policy]

ENFORCEMENT

Failure to comply may result in the following:

1. Computing services or devices may be denied access to UW-Madison information resources.
2. UW-Madison employees may be subject to disciplinary action up to and including termination of employment.
3. Contractors or associates may be subject to penalty under the governing agreement. Compliance may be a consideration affecting new or renewed agreements.

CONTACT

TBD [will depend upon who issues the policy]