# The University of Wisconsin-Madison

# Cybersecurity Risk Management Policy

January 15, 2018

as approved by the Information Technology Committee on January 19, 2018.

## POLICY

~~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.~~

Cybersecurity risk will be managed to ensure that the likelihood and impact of threats and vulnerabilities are minimized to the extent practical. Guided by the Principles below, the focus of this policy is the protection of University ~~information or~~ data and the associated information system~~s. 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,~~ process described in the Implementation ~~Procedures~~ Plan 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 University research, teaching and learning, or administration. Data not owned by the University may fall within the scope of this policy if the data is stored or processed using University assets.

The initial process and any future revisions of the process will be reviewed and approved by IT ~~governance~~Governance[1]. Any IT governance group or the Office of Cybersecurity may initiate a revision by contacting the Policy Analysis Team who will engage IT Governance.

The process will be phased in. Restricted Data systems will be first, with Sensitive and Internal and then Public 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.

Research, teaching and learning, or administrative systems that have a short life span (less than one year) and present a low risk, or that temporarily present a moderate risk, may be granted a temporary exception by registering and describing the system through the Risk Management Framework package intake process, or its successor or designee. Each system will be evaluated on a case-by-case basis to determine the system risk category, the estimated duration of the risk, and if granted, the duration of the exception.

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

---

1 IT Governance is defined at https://it.wisc.edu/it-community/governance/

## 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 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 help protect the integrity and reputation of the University, and provide a secure and safe computing environment for teaching, research, and outreach ~~as well as to protect the integrity and reputation of the University~~.
2. We understand the value of University information as a product of research, ~~data related to~~ teaching, and learning, ~~along with~~including the personal data of our faculty, staff, and students~~students, faculty, researchers, and administrative staff~~.
3. We are committed to ensuring the appropriate security of all data, specifically ensuring that faculty, staff, and student data~~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~~of faculty, ~~students,~~ staff, students, and other members of our community.
5. We ~~will~~ ensure that risk analysis tools and active filtering methods ~~will be~~ are used only for the detection of malicious activity, and are not used for examining any other content in the data stream.
6. We evaluate the content of system~~s~~ 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, vulnerabilities, and compromises. Any personal or private ~~message~~ content captured during the testing and detection process~~es~~ is ignored, and is either not recorded at all, or is eliminated immediately in cases where temporary recording is technologically 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 process allows for temporary situations where immediate defensive action is needed, and reviews those temporary measures to determine if they should become ongoing. ~~processes:~~

   ~~a. Allows 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. We implement prevailing cybersecurity practices that reduce or eliminate the potential for impacting Availability, Integrity or Confidentiality of data and information systems.
9. The procedures that implement the Risk Management Framework~~framework~~ are developed with collaboration in mind and will be revised collaboratively as conditions warrant.

## BACKGROUND

Cybersecurity is a collective responsibility which requires policy that applies to all components of the University of Wisconsin-Madison. Threat, vulnerability and likelihood of exploitation are complex and unique to specific business processes and technologies. Cybersecurity risk is measurable depending on quantified or classified aspects of the data; characteristics of the information system; the definitions and characteristics of internal or external threat, system or environmental vulnerabilities; and the likelihood that the event or situation may manifest itself within a given application, information system or architecture. External threats evolve rapidly and are persistent based on the criminal intent or the resources of the attacker, whether they are criminal or nation state backed. Internal threats can be accidental or intentional.

The impact of using diverse but competing approaches in implementing security controls applied to information systems tends to elevate overall cybersecurity risk[2]. The management of cybersecurity risk will use a detailed Risk Management Framework~~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.

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

---

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

1. The University 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 the University's mandatory and universally applicable process for managing cybersecurity risk. The process can be tailored to specific technologies, processes, or services.
~~This process can be tailored to specific technologies, processes or services. This policy applies to University 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.).~~
3. The process must include policy and procedural controls to ~~assure~~ensure that privacy and academic freedom are respected.

~~A separate Implementation Plan is attached to the Policy and with additional details related to training, timelines, and processes.~~

## AUTHORITY

This policy was approved by the Information Technology Committee on January 19, 2018 and forwarded to the University Committee. It was presented to the Faculty Senate on February 5, 2018 for information, and issued by the Vice Provost for Information Technology on February 9, 2018.

## ENFORCEMENT

Failure to build and maintain information systems that adhere to the policy and principles in the policy or which significantly deviate from the Implementation Plan will likely increase risk to University data and information systems. Significant architecture, development or operating and process deviations which result is elevated risk or which impact compliance~~comply~~ may result in the following:

1. Computing services or devices may be denied access to University information resources.
2. University 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

Please address questions or comments to the Office of Cybersecurity at cybersecurity@cio.wisc.edu.