# Technology Advisory Group Proposal/Discussion Item

| | | | | | |
|---|---|---|---|---|---|
| **TAG:** Research | **Topic:** | UW-Madison Cybersecurity Risk Management Policy | | | |
| **Date:** November 15, 2016 | **Type of Proposal:** | Technical | Policy | Initiative | |
| **Originator:** Bob Turner, Chief Information Security Officer | 1st Endorser: N/A | 2nd Endorser: N/A | 3rd Endorser: N/A | | |
| **Final Approval Required:** | CIO | ITC | ITSC | University Committee | Chancellor/Provost |
| **Reviewed by MIST** √ | **Other TAG Approvals:** | Infrastructure (Pending) | Divisional (Pending) | Teaching and Learning (Pending) | |

**Executive Summary**: This Policy is needed for well-regulated and managed Risk Management Framework to assess impact of cybersecurity risk on the university community.

**Context (history/threat/etc.)**: University information systems and networks are being targeted by criminals and other threat actors who seek to:

- damage information systems, deny services and disrupt university operations;
- exploit the value of administrative data (i.e., student information, personally identifiable information, other human resources data or medical related information); or
- steal valuable intellectual capital.

The potential for a Restricted or Sensitive data breach or damage to information systems is a University wide risk management problem which could result in financial, operational or reputational harm.

Another significant risk is non-compliance with information security requirements in Federal research grants. Beginning in 2014, Federal agencies providing research funding and grants introduced new requirements based on assessments of emerging threat activities, to include the introduction of: enhanced Federal Information Systems Management Act (FISMA) metrics; a proactive vulnerability scanning process; and updated incident response procedures. Research contracts are now being renewed with emphasis on the enhanced FISMA compliance language.

In order to address these issues, the Office of Cybersecurity developed a Cybersecurity Risk Management Policy which is based on an industry accepted Risk Management Framework. When implemented, this policy will provide a process to materially reduce risk and assure complance with FISMA requirements imposed on grantors. The cost of enacting this policy is a shared responsibility between the Office of Cybersecurity and system owners. Distributed academic and business unit Risk Analysts can be trained by the Office of Cybersecurity or be provided at cost within an agreed level of effort. Risk Executives will need to be designated for each College and Department or business unit. The Risk Executive is an executive or director within the academic or functional unit or in the line of authority above that unit with the authority to accept the risk of operating the system on behalf of the institution. The Risk Executive balances the business needs, the potential financial and reputational cost of adverse events, and the cost of reducing the likelihood and severity of those events.

The Risk Executive must be able to:

a. accept the risk as certified by the Office of Cybersecurity, or
b. assure that action is taken to reduce the risk to an acceptable level, or
c. decline to operate the system.

**Issues and Questions for TAG**:

1. Is the policy easy to understand? If not, which areas need clarification?
2. Does DTAG agree with the content and intent of the policy?
3. Will the DTAG endorse the policy to the IT Council?

# Technology Advisory Group Proposal/Discussion Item

**Background**:

This policy was originally brought before the MTAG in May 2016 as a proposal. The proposal was endorsed to the IT Council for further discussion and presentation to the UC. With the changes in IT Governance currently in progress, a full version of the policy is being presented for review and approval.

The management of risk must address both academic and business needs, the potential impact of adverse events, and the cost to reduce the likelihood and severity of cybersecurity events.

The process described in this policy is a tool used to arrive at an understanding of risk involving information systems. Risk can be modeled as the likelihood of adverse events over a period of time, multiplied by the potential impact of those events. Risk cannot be reduced to zero. There is always a level of risk that must be accepted as a cost of doing business. Reducing the risk to an acceptable level is also a cost of doing business.

Systems are monitored to assure that the level of cybersecurity risk is maintained at or below an acceptable level. There are policy and procedural safeguards to assure that personal privacy and academic freedom are respected. The content or use of the data is only of interest to the extent that it indicates the presence of a vulnerability or threat, such as incoming data that is part of an attack on university systems, or outgoing data that indicates a system has already been compromised. University or personal data that is stolen by an attacker is no longer private. Scrupulous monitoring helps protect data from unscrupulous use.

**Guiding Principles For Implementation**:

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 activity analysis employed for network defense against cybersecurity threats by using Advanced Threat Protection (ATP) tools can have a significant chilling effect on learning and academic freedom, Office of Cybersecurity will operate under the following principles guiding the deployment and use of these systems:

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. Our deployment and use of ATP tools preserves and strengthens the privacy and academic freedom for faculty, students, staff, and members of our community.

3. We will ensure active filtering methods will trigger only upon the detection of malicious activity, not upon any other content in the data stream.

4. 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. ATP is not used to monitor individual activity. Data generated or collected which may identify individual behavior will be retained no longer than is necessary to identify and evaluate malicious traffic.

    b. Data generated by ATP is used only to detect threats and compromises. Any message content captured during the detection process is ignored and either not recorded at all, or eliminated immediately in cases where temporary recording is necessary technologically.

c. Data collected by ATP tools 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.

5. 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.

| **Supporting Materials** | **Attached / Link**: |
|---|---|
| 1. Final Draft - Cybersecurity Risk Management Policy | 1. Attached |
| 2. NIST 800-37 Rev 1 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* | 2. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf |
| 3. NIST 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* | 3. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf |
| 4. RMF Infographic | 4. Attached |

**Short Description of Important References/Supporting Materials**

1. The Draft Cybersecurity Risk Management Policy provides background information on risk management; principles for protecting privacy and academic freedom during risk assessments, data gathering, monitoring and analysis; and policy for managing cybersecurity risk.
2. The two NIST 800 series publications are used as references for developing this policy and for guiding the UW-Madison Cybersecurity Risk Management program and processes. The requirements and processes provided in these U.S. Department of Commerce publications are tailored significantly to address the higher education environment while ensuring compliance with FISMA concepts and requirements.
3. The Risk Management Framework Infographic is a helpful guide that describes the six steps in determining and monitoring information system security controls.