Cybersecurity Strategy 2023-2025

Executive summary

Malicious actors across the globe work relentlessly to adapt and evolve their cybersecurity attack tactics, putting UW–Madison's data, systems, and digital assets at risk. To reduce our risk, UW–Madison's Cybersecurity Strategy must also continually adapt and evolve.

The framework for our Cybersecurity Strategy is formed by an “AIC Triangle” of foundational principles:

- **Availability** of information and systems to those authorized to use them
- **Integrity** to maintain the accuracy and trustworthiness of data across its lifecycle
- **Confidentiality** measures to protect sensitive information from unauthorized access

As we execute these principles, cybersecurity should not be shrouded in mystery to our university colleagues and partners. In our Cybersecurity Strategy, we aim to be transparent and collaborative—a valuable resource in our work to reduce risk and cyber threats to UW–Madison. We do this by offering outreach and service to our university communities—including education, risk assessment and policies. We also want to help our UW colleagues identify and adopt technologies that reduce cyber risk, we also provide a consolidated catalog of the vetted and approved tools and services people need to do their work in pursuit of UW's missions.

A successful Cybersecurity Strategy requires everyone at UW–Madison to be a cybersecurity steward. To forge this critical partnership and support the vision of comprehensive cybersecurity across the university, our strategy involves continuing to strengthen relationships with researchers, faculty and all our campus partners.

We foster academic freedom, research integrity, education, and outreach by providing recommendations to protect assets from unauthorized access, loss, alteration or damage that could adversely affect the university’s reputation. Our challenge is providing robust security while supporting the open information-sharing needs and culture of the academic and research environment.

The Office of Cybersecurity and UW–Madison community join with university leadership to continually improve this strategy. We are guided by the standards set forth in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and work in conjunction with the UW System Information Security Program and Policies.

Mission statement

To defend the university’s digital assets from internal and external threats by deploying risk-based measures.

---

1 UW System Information Security Program, June 25, 2022
Vision statement

An agile, secure, and resilient cyber environment that empowers the UW–Madison community to innovate and achieve the university’s mission: teaching, research, living, community, and performance.

Equity, diversity, inclusion

Diversity is a source of strength, creativity, and innovation for UW–Madison. We value the contributions of each person and respect the profound ways their identity, culture, background, experience, status, abilities, and opinions enrich the university community. The cybersecurity community believes that diversity, equity, inclusion, and inclusive excellence are the four essential pillars of our approach to generating positive and lasting change while building upon the university’s reputation as a leading educational and research institution.

Strategic goals

The Office of Cybersecurity aligns its work to support the mission of the university and the mission of DoIT. The following strategic goals represent a multi-year effort that will unify campus efforts around a single concept: Security controls and processes are managed by people and technology.

The Cybersecurity Team has a significant, key role in helping to protect the reputation of the institution and the privacy and academic freedom of faculty, staff and students. The Office of Cybersecurity cannot do it alone. Every person who uses data and IT services, on campus or remotely, has a role.

Goal 1: risk-based approach

The Risk Management Framework, adopted in 2018 as part of the Cybersecurity Risk Management Policy, establishes a risk-based approach to IT security. This framework enables school, college, and division risk executives to make informed decisions and accept, reduce, transfer or reject the risk of the systems under their responsibility. To ensure proper risk management, it is essential for the university IT Community to join with academic, research, administrative and other stakeholders to collaborate, identify and support requirements, needs, and processes for systems and data.

Cybersecurity to the Edge is an initiative inspired by the need to have a comprehensive university plan for detecting and managing cybersecurity threats. UW–Madison leadership has invested significantly to ensure we protect data and operations using these principles:

- The security framework should extend across the entire university and be applied consistently. The fundamental components of cyber hygiene should be systemically instituted and understood across the university.
- Best practices of care, when those standards are developed, will be maintained, and applied to systems and endpoints accessing university resources and data.
- Employ industry-standard tools and techniques to collect information about campus devices, to include endpoint devices, servers, and network devices.
- Educational programs are tailored to ensure savviness against cyber threats.

---

2 https://policy.wisc.edu/library/UW-503
3 As described by the Center for Internet Security at https://www.cisecurity.org/blog/how-to-implement-assess-your-cyber-hygiene/
4 https://it.wisc.edu/services/endpoint-management/
Goal 2: operational excellence

Proactively eliminating complications in university systems and processes enhances security, operations, and effectiveness in supporting the mission of the university. It is also important to invest in training and certifications for cybersecurity and IT staff to ensure their proficiency in using the tools and analyzing the results.

- Maintain a high-functioning cybersecurity operation across the university that supports the key mission of teaching, learning, research, and community engagement.
- Streamline outdated processes and procedures to incorporate the use of shared services across UW–Madison and UW System.
- Partner with the campus developer community to enhance security.
- Identify and provide common systems to ensure a consistent and adequate approach to cybersecurity across the university.
- Provide outreach and support to smaller IT units for deploying services and implementing best practices.

Goal 3: service management

We must create efficiencies within UW–Madison that help us reduce cybersecurity risk while continuing to build, align, and follow best practices for cybersecurity services and tools by proactively collaborating with distributed IT staff while supporting the University mission.

- Establish a service model that meets the complex needs of the university.
- Continue to discover and review tools that secure and protect data for use by campus partners.
- Create a community of practice to identify ways to make the best use of the tools. Concepts, methods, implementation strategies, and ease of use should be general enough to apply universally and encourage widespread adoption.
- Help to ensure compliance with UW System standards will respect the needs of UW-Madison faculty, staff, students, and researchers in their efforts towards the university mission.

Goal 4: data framework

The success of university colleges, schools, and administration depends on the confidentiality, availability, and accuracy of the information collected and stored. The university will always be susceptible to risk when cultivating and leveraging personally identifiable information about students and employees, intellectual property, and human subject research data, among many other examples of data sets. Risks associated with data loss, misuse, and violations of federal and state laws and regulations are reduced when cybersecurity controls are implemented and maintained. To further address data risk, campus cybersecurity and information technology professionals must maintain a strong partnership with the Office of Data Management and Analytics (ODMAS), campus institutional review boards, Legal Affairs, and Research Data Services.

- Coordinate with university partners to review and update the campus data classification policies, standards, and practices. This includes promoting awareness and training for how to classify and protect data.
- Support the existing campus data privacy program that informs data subjects on what types of data is collected, how it is used, how it is shared, and how long the data should persist in our systems.
- Ensure data platforms provide the controls that secure appropriate access to the data, that the data is available, and that information is secure against loss or destruction.
Goal 5: transparency

Transparency among both internal (all campus divisions and departments) and external partners (UWSA, etc.) is necessary to build trust, to enhance communication and to facilitate understanding of cybersecurity risk. Transparency can be achieved through clear documentation, regular communication, setting good expectations and engaging all stakeholders in the decision-making process. While the nature of security requires that some matters be kept confidential, transparency requires communicating the reasons for confidentiality. The Traffic Light Protocol should be used and respected where appropriate.

- Continue to strengthen relationships by freely sharing information, plans and processes with our partners, internal and external to the university, as appropriate.
- Create a structure for distributing information to campus from our information sharing groups.
- Provide dashboards on campus security posture and cybersecurity risks.
- Develop documentation on what data the cybersecurity tools are gathering, how it is stored, who can access it and when someone would access it.

Goal 6: outreach and service

Outreach and service are integral parts of developing cybersecurity awareness and building a successful, cybersecurity-aware community throughout the UW–Madison campus and the State of Wisconsin. As cybersecurity professionals across UW–Madison, we will partner with stakeholders across campus, the community and the State of Wisconsin to champion educational experiences and cybersecurity awareness while focusing on inclusion, diversity, and equity.

- Provide direct outreach and inclusive education, awareness, and training to UW–Madison faculty, staff, and students
- Provide education, awareness, and training materials in accessible languages and formats
- Participate in career development events designed for students that introduce cybersecurity as a career, particularly focusing on those that are underrepresented in cybersecurity.
- Continue efforts to create an understanding of how to apply the risk management framework to enhance school/college/division risk executives’ decision-making process.

---

5 The Cybersecurity Infrastructure Agency Traffic Light Protocol can be found at [https://www.cisa.gov/tlp](https://www.cisa.gov/tlp)
6 Examples include but not limited to UW-Madison Communities of Practice, Research and Education Networks-Information Sharing and Analysis Center (REN-ISAC), Madison Information Security Team (MIST), Technology and Information Security Council (TISC)