VERSION 2.0 – 25 June 2022

UNIVERSITY OF
WISCONSIN SYSTEM

Information Security Program

TABLE OF CONTENTS

LIST OF TABLES / FIGURES

.

1.0 Document Control

1.1 Document History

Table 1. Versioning

Version	Description of Revision	Written / Reviewed by:	Approved by:	Date:
2.0	Updated Revision	Office of Information Security	Edward Murphy	07/11/2022
1.0	New Document	UW System	Katherine Mayer	04/23/2018

1.2 Executive Sponsor Review and Approval

Table 2. Sponsor Review and Approval

Name	Role	Date
James Langdon	Vice President for Administration	08/10/2022

1.3 Stakeholder Endorsement

Table 3. Stakeholder Review and Endorsement

Name	Role	Date
UW System Chief Information Officer Council	Campus CIO Perspective	06/25/2022
UW System Technology & Information Security Council	Campus Information Security Officer (ISO) Perspective	06/21/2022

1.4 Related Documents

Table 4. Related Documents

Document Name	Date
UW System Regent Policy Document 25-3, Acceptable Use of Information Technology Resources	10/6/2017
UW System Regent Policy Document 25-4, Strategic Planning and Large or High Risk Projects	7/9/2021
UW System Regent Policy Document 25-5, Information Technology: Information Security	2/5/2016

.

2.0 UW System Information Security Program

The purpose of this University of Wisconsin (UW) System information security (IS) document is to continue development and maintenance of *an enterprise, systemwide program* designed to ensure the confidentiality, integrity, and availability of UW System Administration and institutions' information assets from unauthorized access, loss, alteration, or damage while supporting the open, information sharing needs of the academic environment. A robust information security environment is critical to enabling the UW System mission of developing human resources, discovering, and disseminating knowledge, and extending knowledge and its application beyond the boundaries of its institutions.

The UW System Information Security Program provides a structure for developing and maintaining *systemwide security policies and standards* as the basis to assure information security for all UW institutions and defines the fundamental principles for the protection of UW information assets, and the proper controls needed to ensure compliance with internal and external regulations to uphold UW System's security posture and reputation. Additionally, this program provides the baseline to evolve and mature a risk assessment and management approach that integrates risk identification and appropriately prioritized mitigation strategies that reasonably protect the critical information assets, infrastructure, and services of highest value.

The Information Security Program states UW System Administration's (hereafter referred to as "UWSA" or "UWSA's") responsibility for securing the information assets of the UW System and its delegation of that responsibility to UW System institutions (hereafter referred to as "institution" or "institutions").

The UW System Information Security Program is guided by the standards set forth in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which is widely adopted across both public and private sector organizations, throughout the United States. The NIST CSF provides a policy framework for cybersecurity management, including asset identification, systems protection, threat detection, incident response, and recovery. Specifically, the UW System Information Security Program leverages NIST Special Publication 800-53, which covers the steps in the framework that comprehensively address security controls across multiple areas of information security.

3.0 Scope of the Program

The concepts, policies, standards, and initiatives within this Information Security Program apply to *UWSA and all UW institutions*. All *must comply with the enterprise, systemwide information security program, policies, and standards* as reviewed, approved, and signed by the President and the Vice President for Administration.

Each member of the UW System community is responsible for the security and protection of information assets over which he or she has control. The UW System community is defined as students, faculty, staff, 3rd party vendors, visiting scholars/lecturers, and/or units and other persons who are acting on, for, or on behalf of the UW System and its institutions. Resources to be protected include but are not limited to all electronic equipment, facilities, access/control systems, technologies, and data used for information processing, transfer, storage, display, printing, and communications by the UW System community, as well as services that are owned, leased, operated, provided by, or otherwise connected to UW System resources. The physical

.

and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise.

Unless specified otherwise by systemwide policy, standard, or procedure, UWSA and the institutions can develop more stringent local policies and procedures that address specific local issues. UWSA and the institutions may develop policies and procedures tailored to their environment that address areas not covered by systemwide policies. *If UWSA or an institution chooses to keep or develop information security policies, standards, or procedures of its own, those products are valid only to the extent that they are more stringent than the requirements contained in the systemwide policies, standards, and procedures, which constitute the mandatory baseline.*

4.0 Vision and Program Goals

The vision of the UW System Information Security Program is to enable the instruction, research, extended training, and public service of the UW System and its institutions by delivering a robust and reliable information security environment that inspires innovation, collaboration, and trust. The aim of the program is to effectively manage information security risks to its assets and the UW System community through the following over-arching goals:

- minimize data loss or compromise that could otherwise result in significant risk to highly sensitive/personal or institutional data or cause significant reputational harm;
- improve security of critical system and network services through enterprise, defense-in-depth approaches to reduce risks commonly associated with disaggregated computing environments;
- proactively assess, reduce, and manage risk in a manner that enables data/system owners, administrators, and the larger UW System community to be more aware of the risks that their information assets are vulnerable to, identify controls to reduce those risks, and understand the residual risk remaining after any identified controls have been implemented; and
- enhance crisis and information security incident response/management to enable the UW System to quickly recover its information assets in the event of a catastrophic event and to manage information security events more efficiently and effectively, thereby reducing or minimizing the damages to the UW System community.

5.0 Need for Security

The UW System community has an obligation to protect institutional and personal data in accordance with this program and corresponding regulations. This program accounts for the UW System's mission and promotes, supports, and adopts an institutional culture that embraces academic freedom and collaboration within a secure information environment.

Information security threats and threat actors are becoming persistent, sophisticated and agile. They are increasing in volume causing risk management strategies to become more complex. Higher Education is near the top of the cyber criminal's radar and the sense of urgency must translate into proactive actions to protect high risk data, prevent fraud, and mitigate the impacts from ransomware and other forms of malware. Institutions are frequently sought for their valuable research information, intellectual property, assets, personal and healthcare information. This Information Security Program provides a platform to develop effective practices and controls to protect against the ever-evolving threats faced by the UW System.

The current UW IT environment is highly distributed with few standard operating protocols or security controls. Long-term, the best and most cost-effective way to secure the environment is to consolidate and standardize core infrastructure and services. The UW System will remain consistent and adopt a unified approach to information security through a critical initiative called IT as a Service (ITaaS). ITaaS will commoditize and consolidate core IT infrastructure to achieve broader scale, lower costs, and increased quality, while improving our overall security posture by significantly shrinking our attack surface and standardizing operations. Furthermore, ITaaS will improve critical IT workforce risk by establishing multiple teams of IT specialists thereby providing workforce resiliency.

6.0 Roles and Responsibilities

The UW System community is responsible for ensuring that UW information assets are used only in proper pursuit of the university's operations; information is not improperly disclosed, modified, or endangered; and access to university information assets is not made available to unauthorized personnel, information systems, or services.

According to Regent Policy Document 25-5, the Board of Regents delegates to the President of the UW System the authority to implement and maintain an information security program. Each UW System institution shall consistently apply the program and related processes.

The Chancellor or designee, generally the chief information officer, at each UW System institution shall:

- be responsible for compliance with the systemwide information security program and related policies and processes;
- provide information-security-related training and guidance to their respective institutions; and
- collaborate with systemwide information security governance committees to maintain consistent policies, processes, and communications about the UW System information security program.

In order for Chancellors to consistently apply the information security program, on April 4, 2018, the UW System President specified via memo that all information technology (IT) environments at each institution shall be under the oversight of a single person designated by the Chancellor. The designee shall have the responsibility to ensure all IT operations at the institution are conducted in a secure fashion. See appendix A.

Therefore, the Chancellor and their designee at each institution are responsible for ensuring that appropriate security controls are in existence and enforced throughout their respective university. Institution IT (information technology) and IS (information security) teams shall provide appropriate guidance and assistance to their larger institution community to ensure all understand and employ the required controls to protect the information assets within their purview in accordance with this program and supporting UW System information security policies.

Similarities between institution information security organizations can facilitate inter-institutional lines of communication and form a foundational organization and structure that supports the overall goal of improving information security. The baseline roles and responsibilities for each organizational role are described in further detail in the table below. Additional roles and responsibilities may be added or combined based on local needs.

.

Table 5. Roles and Responsibilities

Role	Job Functions	Responsibilities
Institution Chancellor	Assumes high level accountability and responsibility for their institution's compliance with the timely adoption and implementation of the UW System Information Security Program, including empowering the CIO, or other designee, to engage in all necessary activities to implement this program and associated policies and standards across all areas of their institution.	• Conveys priority of information security work to CIO, or other designee, and other institution leadership • Facilitates CIO, or other designee, influence over institution information systems • Resolves high level conflict regarding information security issues • Maintains accountability to the UW System Board of Regents
UW System Associate Vice President (AVP) for the Office of Learning & Information Technology Services (OLITS) and CIO	Leads information technology planning for the University of Wisconsin System, information technology (IT) services delivery to UW System Administration and IT as a Service customers, defining the digital strategy for the system, and ensures effective implementation and management of information technology services.	• Leads the planning and implementation of strategic and core IT initiatives in the UW System including information security, financial, human resource, student information, budget and planning, data analytics, and broadband services • Serves as a resource for institutions and senior UW System administrators for learning and information technology policies, procedures, and practices • Directs the development and implementation of IT policies and procedures for the UW System
UW System Associate Vice President (AVP) for Information Security (OIS) and CISO	Serves as the oversight authority in all matters of information security, across the UW System, including IS services delivery to UW System Administration and the IT as a Service customers, the successful and timely comprehensive deployment and management of the IS Program, policies, and standards throughout all UW Institutions.	• Communicates IS expectations to the CIOs/Chancellor designee • Allocates UW System IS resources accordingly • Resolves high level IS issues • Develops system wide IS policies • Communicates IS matters to the UW System President and Board of Regents
Information Security (IS) Designee / Campus CIO	Leads a customer-focused organization that delivers innovative, efficient, and effective technology solutions to support the teaching, research, and service missions of the UW System and institutions Serves as the institution's single oversight of its information technology environment.	• Advances the technology aspects of important institution initiatives • IT strategic planning and decision management • Supports the research, teaching and outreach mission of UW System and institutions • Ensures all IT operations at the institution are conducted in a secure fashion • Reports status of information security environment, including incidents, to campus and System leadership

.

Role	Job Functions	Responsibilities
Institution Information Security Director / Manager (ISO)	Protects UW System information and its technical infrastructure from external or internal threats and to assure that UW complies with applicable statutory, regulatory and policy requirements. Supports the mission and vision of the UW System and institutions.	• Assesses, manages, and mitigates information security risk • Implements IS policies • Conducts compliance and enforcement activities • Responds to cybersecurity incidents as they occur • Conducts outreach, education, and awareness • Provides guidance to the institution, divisions, departments, and units to meet or maintain compliance with applicable policies, standards, baselines, guidelines, and laws
IS Director	Manages the operation of an information security unit or area including establishing service delivery metrics, assessing unit progress, and accountable for quality of service. Plans, organizes, and controls all aspects of the operation including supervision and scheduling of professional technical staff, prioritizing, and assigning of the work, and coordinating activities with other UW System or institution units.	• Plans, organizes, and controls the operation of complex information security units • Establishes procedures, oversees the acquisition of software and hardware solutions to support unit operations. • Participates in the IS Advisory Council as the Service Owner for all IS services delivered by their unit • Cyber Defense Director plans and organizes incident response annual table top exercise
Cyber Defense Analyst	Performs security operations, information security threat analysis, security incident response activities, and vulnerability management services.	• Monitors alerts and develops security operations plays to continuously advance security event detection and response capabilities. • Conducts vulnerability scans of IT environment to produce prioritized report on top system vulnerabilities • Supports all aspects of security incident response activities • Utilizes various security threat intelligence sources to protect critical IT systems and university operations.
Information Security Analyst	Performs security risk management analysis, policy development and maintenance, audit support, and vendor security management.	• Gathers and analyzes materials about information systems to provide third-party security assessments • Ensures the information security risk management program operations and controls are being consistently performed or applied • Assesses requirements for updates to security policies based on changes to business functions, technical vulnerabilities, and emerging threats.

.

Role	Job Functions	Responsibilities
Security Architect	Assesses the UW System's security strategy, architectures, and practices and translates university objectives and risk management strategies into specific security processes enabled by security technologies and services.	• Advises the university on upcoming and ongoing regulatory changes or status of threat landscape to help university leadership make risk informed decisions. • Develops and maintains a security architecture process and artifacts that can be used to leverage security capabilities in projects and operations. • Tracks changes in digital technology and threat environments to ensure that these are adequately addressed in security strategy. • Validates IT infrastructure for security best practices • Operates as a member of the Enterprise Architecture team
Security Engineer	Supports the information security technology including upgrading, patching, tuning, and developing integrations for all enterprise security systems. Designs, develops, and supports all security orchestration and automation response (SOAR) activities.	• Develops and maintains automated monitoring and detection scripts. • Develops and maintains SIEM integrations. • Configures, tunes, and updates enterprise security solutions.
IT Director	Manages the operation of an information technology unit or area including computer hardware, software, networking, and telecommunications equipment. Plans, organizes, and controls all aspects of the operation including; supervision and scheduling of professional and technical staff, prioritizing and assigning of the work, and coordinating activities with other UW System or institution units.	• Plans, organizes, and controls the operation of complex information technology units • Provides technical support for all hardware and systems software sets standards • Establishes procedures, oversees the acquisition of supplies and equipment schedules • Recommends hardware acquisitions and the acquisition and maintenance of support equipment; works the contracting and procurement of new equipment and software
Risk Manager	At the institution level, manages, develops, and implements System and Institutional risk management programs, policies, and procedures appropriate to the organization. Ensures continuity of cyber liability Insurance program effort with CISO, ISO, Records Manager, and other information security resources. **	• Analyses risks and communicates appropriate responses • Reviews and negotiates contracts as they relate to insurance, indemnification, and liability issues in consultation with Legal Counsel, or UW System Office or Risk Management • Administers and manages university programs: ○ Liability and automobile claims ○ Property insurance claims ○ Loss control programs ○ International safety and security programs

.

Role	Job Functions	Responsibilities
		• Maintains key statistics related to risk management processes, and uses those statistics to continuously improve processes
Security Awareness	The UW System Director of Security Awareness and Outreach leads the system-wide security awareness program.	• Develops and maintains content for employee annual security awareness training. • Plans, conducts and analyses recurring phishing training awareness campaigns.
Records Manager **(Designated as the Records Officer per Wisconsin Statute Wis. Stat. 15.04(1)(j) and Regents Policy 3-2 *Public Records Management*)**	Consults systemwide with all office levels in managing all information assets, regardless of format or medium, in accordance with Records Management Best Practices. Provides consultation on research records and data management issues	• Develops and maintains a public records management program that fulfills state and federal legal requirements • Provides records management training and assistance to institution employees • Upon request, provides special assistance to UW System institution: legal counsel, legal custodians for public records requests, auditors, and archivists • Collaborates with technology professionals in developing and maintaining information and digitization systems that create, receive, store, destroy, and archive electronic public records in compliance with state and federal legal requirements
Data Governance / Data Custodian	Facilitate data-driven decision-making. For users from all departments of the institution to be able to make informed decisions, a culture of information literacy and sharing should be established at the institution level.	• Develops the risk management strategies and compliance with record retention policies for differing record types • Aligns and coordinates with records management to ensure compliance. • Ensures there are common data definitions, and those definitions are made available across multiple data domains to enable informed decision making
Data Steward(s)	Management and oversight of UW System and institution data assets to provide business users with high-quality data that is easily accessible in a consistent manner. Allow for and facilitate data-driven decision making.	• Evaluates and classifies data according to UW System policy and procedure • Facilitates the communication of institutional data-related policies across the institution • Promotes data governance across the institution • Implements major data-related projects • Recommends the need for resources and budget for the implementation of major data-related projects • Monitors key metrics related to the ongoing program operations

.

** Will require system-driven training for the institution risk managers.

7.0 Implementation, Enforcement and Monitoring

UW System Administration and institutions will implement this Information Security Program using enterprise and institutional delivery of services to include an assessment of enterprise security solutions, risks, associated costs, and resource estimates. The institutions top-10 risks as identified in the UW System risk register identify specific tasks and sub-tasks.

Institution Chancellors retain overall responsibility for compliance with this program and related information security policies at their respective institutions. UW System Administration shall support/monitor the institutions for compliance with the Information Security Program, including but not limited to the following activities: designing and developing processes and controls to manage risks; defining how to measure success; and assisting institutions in escalating critical issues and emerging risks.

To ensure the information security program is applied consistently across the UW System as specified by the Regent policy, an on-line survey structure has been developed for UW institutions to report policy compliance on a regular basis. Monitoring is conducted through sharing of reports with UW institutions and UW System leadership, including Internal Audit. This approach is in support of the February 8, 2021, UW System "Information Security Actions" joint letter issued by Andrew S. Petersen, President, UW System Board of Regents and Tommy G. Thompson, President, UW System (appendix B), as well as in response to the Legislative Audit Bureau’s recommendation to ensure all University of Wisconsin institutions comply with its policies and procedures,

8.0 Violation Reporting and Escalation

Failure to adhere to the provisions of this program and supporting information security policies and standards may result in the suspension or loss of access to UW System IT resources; appropriate disciplinary action as provided under existing procedures applicable to students, faculty, and staff; civil action; or criminal prosecution. To preserve and protect the integrity of UW System information assets, there may be circumstances where a UW institution may immediately suspend or deny access to resources.

All personnel covered by this program are obligated to report apparent violations. Any individual who suspects a violation of this program and its supporting policies shall report it to their institution Information Security Officer or alternatively to the UW Administration Deputy Chief Information Security Officer.

9.0 Periodic Review

The UW System Information Security program is intended to be a living document that must be periodically updated to maintain alignment with relevant developments regarding cybersecurity threats, risks, and compliance matters facing the UW System.

The information security program will be reviewed every two years or as required and will be revised based on, but not limited to: updated industry regulations or standards; organizational changes; and/or newly identified risks and threats.

.

10.0 Legal or Regulatory Requirements

The UW System continuously endeavors to comply with the information security requirements and implications of any applicable laws, regulations or standards. Examples of some of the requirements include the following: 20 U.S.C. § 1232g, Family Educational Rights and Privacy Act (FERPA); Pub.L. 104-191, Health Insurance Portability and Accountability Act (HIPAA); Pub.L. 106-102, Gramm-Leach-Bliley Act (GLBA); Section 134.98, Wisconsin Statutes, Notice of unauthorized acquisition of personal information; and Payment Card Industry (PCI) Data Security Standards.

11.0 Information Security Policies

The baseline policies, standards, and procedures regarding information security are numbered within the 1000 series of systemwide policies that are available on the UW System Administrative Policies and Procedures website.

11.1 Information Security Policies, Standards and Procedures

An information security policy is typically a document that outlines principles that must be met and are specific to a particular topic or area. Standards and procedures normally contain specific requirements that must be met by institutions. Guidelines can be adopted based on specific technologies or unique work processes.

A comprehensive set of policies and procedures have been developed and are maintained consistent with the five core functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): identify, protect, detect, respond, and recover.
UW System continues to mature its IT security program via revision of existing as well as the publication of several new information security (IS) policies. This policy set, including supporting procedures, is well-aligned with the NIST's CSF and substantially improves the UW System's ability to identify, protect, detect, respond, and recover from IS threats and associated incidents.

11.2 Information Security Policy Development

The overall process for developing finance and general administration policies within the systemwide UW System Administrative policy series that cover the entire UW System is illustrated below in Figure 1.

.

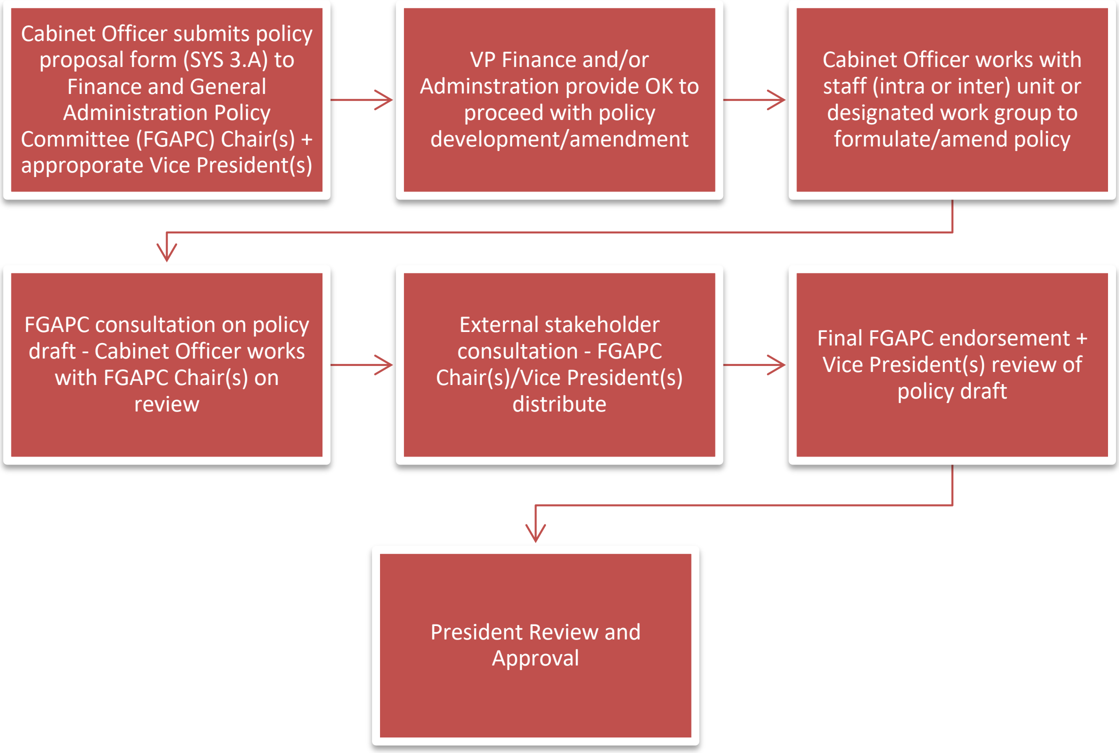

Cabinet Officer submits policy proposal form (SYS 3.A) to Finance and General Administration Policy Committee (FGAPC) Chair(s) + approporate Vice President(s)
VP Finance and/or Adminstration provide OK to proceed with policy development/amendment
Cabinet Officer works with staff (intra or inter) unit or designated work group to formulate/amend policy
FGAPC consultation on policy draft - Cabinet Officer works with FGAPC Chair(s) on review
External stakeholder consultation - FGAPC Chair(s)/Vice President(s) distribute
Final FGAPC endorsement + Vice President(s) review of policy draft
President Review and Approval

Figure 1: UW System Administrative Policy Development Process

Note: Approval process for UW System Administrative Policies and Procedures is outlined in Operational Policies 1-3 and in their associated procedures. However, Presidential approval is not required for procedures. Vice Presidents can approve procedures.

The review processes for General Administration Policies and Procedures are outlined in Administrative policies established by the Office of Academic and Student Affairs, Office of Administration, and the Office of Finance. These policies and any subsequent revisions to these policies, are subject to the approval of the UW System President.

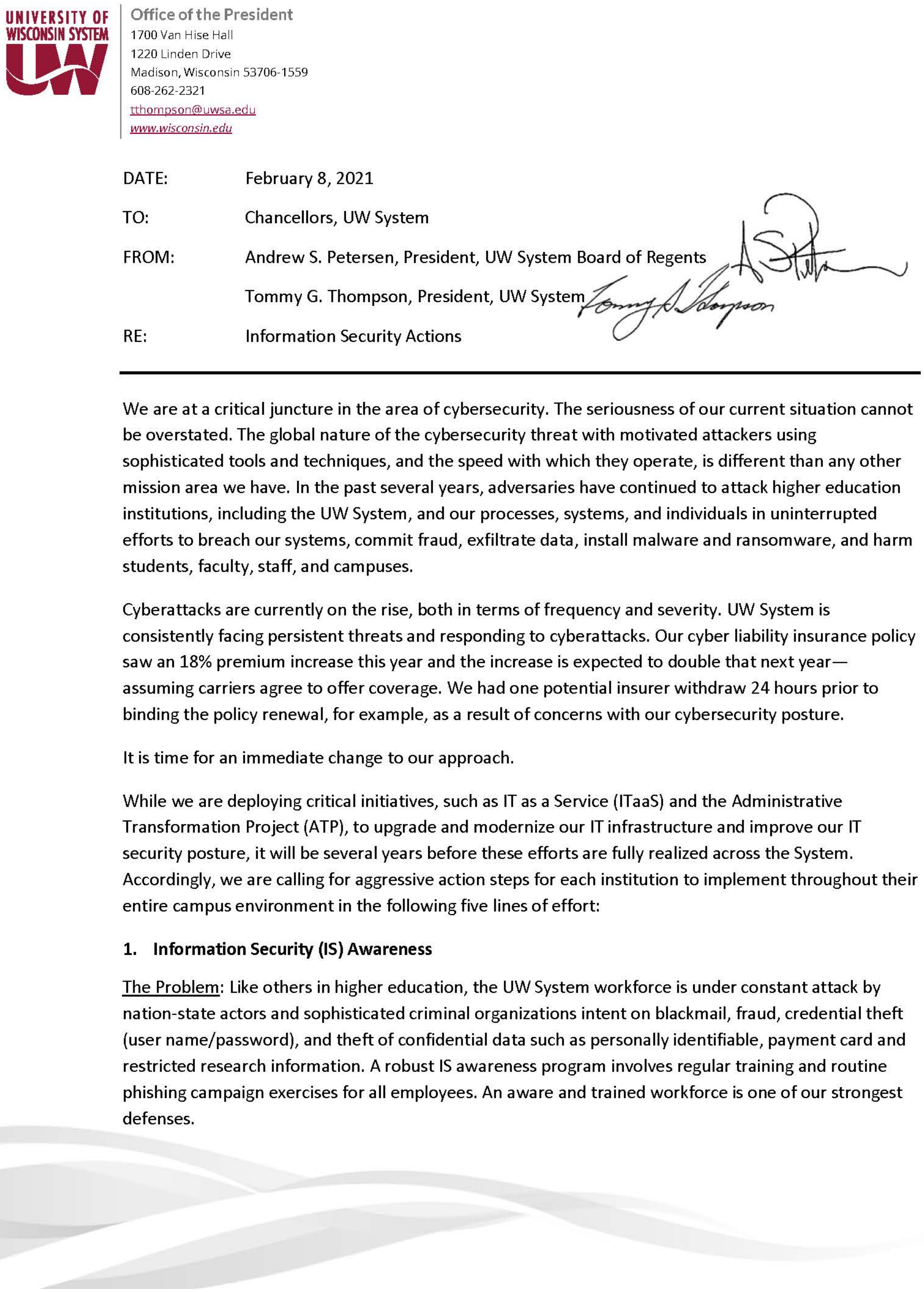
The development or revision of administrative policies and procedures must include the opportunity for appropriate levels of consultation with affected stakeholders, and a date upon which the policy will be reviewed by individuals or groups charged with reviewing administrative policies and procedures. Administrative policies and procedures are to be developed in alignment with all laws, regulations, Regent Policy Documents, and other applicable policies and procedures.

The UW System President approves all UW System Administrative Policies. All procedural documents associated with administrative policies are approved by the appropriate Vice President, as determined by the nature of the procedures being considered. The Office of the President shall serve as the custodian of UW System policies and procedures and work with relevant offices at UW System Administration to ensure the timely communication and publication of all approved policies. This responsibility is currently performed by the Director of Administrative Policies and Special Projects, who reports to the UW System Vice President for Administration.

.

Appendix A: UW System President and Board of Regents President Memo of 8 February 2021

.



Office of the President
1700 Van Hise Hall
1220 Linden Drive
Madison, Wisconsin 53706-1559
608-262-2321
tthompson@uwsa.edu
www.wisconsin.edu

DATE: February 8, 2021

TO: Chancellors, UW System

FROM: Andrew S. Petersen, President, UW System Board of Regents
Tommy G. Thompson, President, UW System

RE: Information Security Actions

We are at a critical juncture in the area of cybersecurity. The seriousness of our current situation cannot be overstated. The global nature of the cybersecurity threat with motivated attackers using sophisticated tools and techniques, and the speed with which they operate, is different than any other mission area we have. In the past several years, adversaries have continued to attack higher education institutions, including the UW System, and our processes, systems, and individuals in uninterrupted efforts to breach our systems, commit fraud, exfiltrate data, install malware and ransomware, and harm students, faculty, staff, and campuses.

Cyberattacks are currently on the rise, both in terms of frequency and severity. UW System is consistently facing persistent threats and responding to cyberattacks. Our cyber liability insurance policy saw an 18% premium increase this year and the increase is expected to double that next year—assuming carriers agree to offer coverage. We had one potential insurer withdraw 24 hours prior to binding the policy renewal, for example, as a result of concerns with our cybersecurity posture.

It is time for an immediate change to our approach.

While we are deploying critical initiatives, such as IT as a Service (ITaaS) and the Administrative Transformation Project (ATP), to upgrade and modernize our IT infrastructure and improve our IT security posture, it will be several years before these efforts are fully realized across the System. Accordingly, we are calling for aggressive action steps for each institution to implement throughout their entire campus environment in the following five lines of effort:

1. Information Security (IS) Awareness

The Problem: Like others in higher education, the UW System workforce is under constant attack by nation-state actors and sophisticated criminal organizations intent on blackmail, fraud, credential theft (user name/password), and theft of confidential data such as personally identifiable, payment card and restricted research information. A robust IS awareness program involves regular training and routine phishing campaign exercises for all employees. An aware and trained workforce is one of our strongest defenses.

Actions Directed:

- Each institution will be fully compliant with UW System Administrative Policy 1032: Information Security: Awareness by July 1, 2021.
- UW System Administration (UWSA) will conduct monthly phishing campaign exercises with employees and record and track results.
- All employees must take these efforts very seriously and meet the expected training and performance standards. For any employee who fails to take annual security awareness training and/or for any employee who fails phishing campaign exercises three times in a given year, the university will suspend their network account access. Network account access may be restored only upon successful completion of the annual security awareness training, or in the case of phishing failures, upon successful completion of supplemental phishing security training.

2. Remote Access

The Problem: Recent external scans, security risk assessments, and cyber incidents have identified the widespread practice of remote access providing access to critical infrastructure, administrative systems, and faculty/staff workstations directly to the internet with minimal authentication requirements.

Actions Directed:

- Each UW institution will close off all remote access points that are exposed directly to the internet, where possible.
- Recognizing the legitimate operational need to allow remote access to certain IT systems while also reducing the attack surface that direct remote access provides, UW institutions will implement an additional layer of defense for any remote access that cannot be closed off.
- Each institution will complete the above actions by December 31, 2021.

3. Disaster Recovery

The Problem: Ransomware attacks are on the rise and disrupt operational activities by encrypting all computing devices in the impacted environment. One of the best defenses against such attacks is the availability of current, comprehensive, off-line backups for quick recovery.

Actions Directed:

- Each UW institution will develop a plan to fully back up all high-risk data at least once every 28 days. Additionally, these backups will be tested at least once every 90 days.
- Each UW institution’s backup and testing plan will be documented by March 31, 2021. The plan will include detailed implementation timelines that will result in full compliance by no later than July 1, 2021.

4. Information Security Performance Management

The Problem: The cyber risk to digital assets across the UW System, both cloud and on-premises, may not be visible, whether that’s due to lack of the right tools, expertise, capacity, or other reasons. This lack of visibility leads to a greater likelihood of suffering a breach that negatively impacts operations, financials, and the reputation of UW System institutions.

Actions Directed:

- UWSA will procure a third-party solution to assign security ratings (grades) by institution, and institutional unit (schools/colleges, centers, etc.) to help monitor progress in meeting goals. Reports will cover several categories such as user behavior, open ports, compromised systems, and other metrics which accurately describe/assess the institution's cyber risks.
- Reports will be delivered to each Chancellor on a monthly basis, as a foundation for developing the appropriate remediation or other actions.
- UWSA will collaborate with each institution to develop targeted metrics and deadlines.

5. Accountability

The Problem: The Board of Regents delegates to the President of the UW System the authority to implement and maintain an information security program. Each UW System institution, however, is responsible for implementing the information security program and for compliance with the systemwide information security policies and procedures. Additionally, institutions have not consistently implemented a structure to evaluate cybersecurity risk and set accountability for management and mitigation of these risks, and this must be addressed.

Actions Directed:

- By March 1, 2021, each UW institution will reaffirm its IS Designee who is responsible for the information security of their entire institutional environment. The name of the IS Designee should be sent in an email to Vice President James Langdon and Associate Vice President Kathy Mayer.
- By April 1, 2021, UWSA will develop data elements required in a monthly report that each institution will provide to its Chancellor and to UWSA (Office of Internal Audit and Office of Information Security). Expected data elements may include:
  - Status of compliance with existing IS policies
  - Status of progress or completion of actions identified in this memo
  - Description of cybersecurity incidents
  - Others as required.
- Each UW institution will begin monthly reporting effective July 1, 2021.

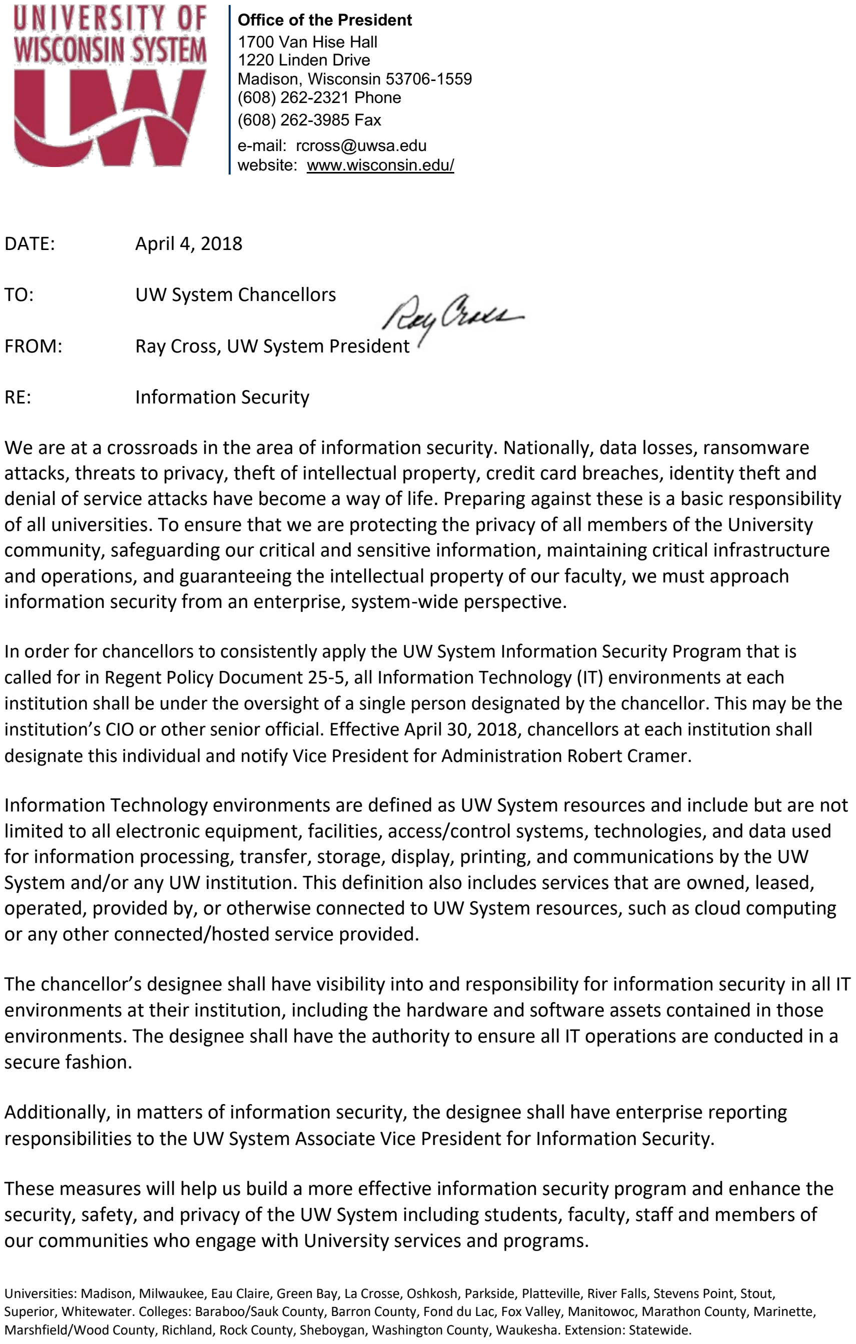
We appreciate the commitment that you and your universities have shown to ensuring our information security in the UW System. The challenges are great and so is the need. Together, we will address these vital issues.

To expedite progress, we are expecting the actions identified in these five lines of effort to be completed by the indicated dates. To validate progress and completion of these actions, we will leverage UW System's Internal Audit Team and appropriate external partners.

Cybersecurity is an important area of focus for all of us in the UW System. As mentioned, we are in the process of developing a transition plan to migrate all the comprehensive universities to ITaaS by July 1, 2024. Until then, however, these actions – and likely others to follow – will help us build a more effective cybersecurity program and reduce risk by enhancing the security, safety, and privacy of the UW System including students, faculty, staff and members of our communities who engage with University services and programs.

While there is no such thing as perfect protection, the current risk balance is off. It is time to balance the scale. We look forward to your partnership and shared commitment to strengthening our cybersecurity posture and reducing risks associated with a multitude of ever-persistent threats.

Appendix B: UW System President Memo of 4 April 2018



UNIVERSITY OF WISCONSIN SYSTEM

Office of the President
1700 Van Hise Hall
1220 Linden Drive
Madison, Wisconsin 53706-1559
(608) 262-2321 Phone
(608) 262-3985 Fax
e-mail: rcross@uwsa.edu
website: www.wisconsin.edu/

DATE: April 4, 2018

TO: UW System Chancellors

FROM: Ray Cross, UW System President Ray Cross

RE: Information Security

We are at a crossroads in the area of information security. Nationally, data losses, ransomware attacks, threats to privacy, theft of intellectual property, credit card breaches, identity theft and denial of service attacks have become a way of life. Preparing against these is a basic responsibility of all universities. To ensure that we are protecting the privacy of all members of the University community, safeguarding our critical and sensitive information, maintaining critical infrastructure and operations, and guaranteeing the intellectual property of our faculty, we must approach information security from an enterprise, system-wide perspective.

In order for chancellors to consistently apply the UW System Information Security Program that is called for in Regent Policy Document 25-5, all Information Technology (IT) environments at each institution shall be under the oversight of a single person designated by the chancellor. This may be the institution's CIO or other senior official. Effective April 30, 2018, chancellors at each institution shall designate this individual and notify Vice President for Administration Robert Cramer.

Information Technology environments are defined as UW System resources and include but are not limited to all electronic equipment, facilities, access/control systems, technologies, and data used for information processing, transfer, storage, display, printing, and communications by the UW System and/or any UW institution. This definition also includes services that are owned, leased, operated, provided by, or otherwise connected to UW System resources, such as cloud computing or any other connected/hosted service provided.

The chancellor's designee shall have visibility into and responsibility for information security in all IT environments at their institution, including the hardware and software assets contained in those environments. The designee shall have the authority to ensure all IT operations are conducted in a secure fashion.

Additionally, in matters of information security, the designee shall have enterprise reporting responsibilities to the UW System Associate Vice President for Information Security.

These measures will help us build a more effective information security program and enhance the security, safety, and privacy of the UW System including students, faculty, staff and members of our communities who engage with University services and programs.

Universities: Madison, Milwaukee, Eau Claire, Green Bay, La Crosse, Oshkosh, Parkside, Platteville, River Falls, Stevens Point, Stout, Superior, Whitewater. Colleges: Baraboo/Sauk County, Barron County, Fond du Lac, Fox Valley, Manitowoc, Marathon County, Marinette, Marshfield/Wood County, Richland, Rock County, Sheboygan, Washington County, Waukesha. Extension: Statewide.