VERSION 1.0 – 30 April 2018

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:
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
Ray Cross	President	4/27/2018
Robert Cramer	Vice President for Administration	4/27/2018

1.3 Executive Stakeholder Endorsement

Table 3. Stakeholder Review and Endorsement

Name	Role	Date
Robert Cramer	Vice President for Administration	4/27/2018
Katherine Mayer	Associate Vice President for Information Security	4/26/2018
David Stack	Vice President, Learning and Information Technology Services (OLITS)	4/25/201818
Nicholas Davis	Chief Information Security Officer (CISO)	4/23/2018

1.4 Related Documents

Table 4. Related Documents

Document Name	Date
UW System Regent Policy Document 25-5, 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. Appendix A contains a glossary of terms used throughout this document.

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:

- prevent data loss or compromise that could otherwise result in significant risk to highly sensitive/personal or institutional data or reputation;
- 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 what risks remain 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 private data in accordance with this program and corresponding regulations, which account 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. *The UW System will remain consistent and adopt one unified approach to information security across all institutions* while recognizing specific needs of this organizationally and functionally complex environment. This approach includes enterprise oversight with full transparency and understanding of the environment coupled with consistent, systemwide application of security policies and controls. A critical element of our program is not only protection but our readiness to respond and quickly recover to incidents that occur.

Information security threats and threat actors are becoming progressively persistent 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. 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.

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 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 authority to ensure all IT operations at the institution are conducted in a secure fashion. See appendix B.

Therefore, the chancellor and his/her 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, 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 (IS)	Serves as the oversight authority in all matters of information security, across the UW System, including 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 • Approves appropriate mitigating control exception requests • Communicates IS matters to the UW System President and Board of Regents

Role	Job Functions	Responsibilities
UW System Chief Information Security Officer (CISO)	The CISO ensures the development, adoption, implementation, and adherence to the UW System Information Security Program, across all UW System institutions, providing managerial as well as technical consultative direction, necessary to achieve continuous compliance with the UW System Security Program, as well as manage large scale incident response activities, related to cybersecurity events.	• Develops policy and supporting standards in support of the UW System Information Security Program • Evaluates and recommends appropriate technical, physical and administrative controls, in support of the UW System Information Security Program • Communicates expectations to the Information Security Officers (ISOs) on the individual campuses • Provides direction to ISOs and other campus stakeholders on the appropriate implementation of UW System policies and associated standards • Evaluates mitigating control exception requests • Communicates appropriate matters to the UW System Vice President of Information Security
Institution Lead IT Authority as Designated by the Chancellor	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 • Responsible for data governance, architecture, and management • Ensures all IT operations at the institution are conducted in a secure fashion
Institution Information Security Director / Manager (CISO, ISO)	Protects UW System information and its infrastructure from external or internal threats, and to assure that UW complies with applicable statutory and regulatory requirements. Supports the mission and vision of the UW System and institutions.	• Assesses, manages and mitigates information security risk • Develops institutional IS policy • Conducts compliance and enforcement activities • Responds to 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

Role	Job Functions	Responsibilities
IT Security Specialists	Performs security operations, information security threat analysis, and tools maintenance.	• Gathers and analyzes materials about information systems to provide recommendations to improve compliance and achieve greater levels of data and information systems security • Ensures security program operations and controls are being consistently performed or applied • Assesses requirements for updates to security plans based on changes to business functions, technical vulnerabilities, and emerging threats
IT Operations Manager(s)	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 • Installs and de-installs computer hardware; plans and establishes security systems; 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. ****	• Analyzes 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 • Maintains key statistics related to risk management processes, and uses those statistics to continuously improve processes
Records Manager	Consults systemwide with all office levels in managing all information assets, regardless of format or medium, in accordance with Records Management Best Practices.	• Develops and maintains a public records management program that fulfills state and federal legal requirements • Provides records management training and assistance to institution employees

Role	Job Functions	Responsibilities
(Designated as the Records Officer per Wisconsin Statute Wis. Stat. 15.04(1)(j) and Regents Policy 3-2 *Public Records Management*)	Provides consultation on research records and data management issues	• 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. In order 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 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 risks, associated costs and resource estimates. Specific tasks and sub-tasks are identified in this document's accompanying 24-month work plan that is distributed separately.

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, each quarter the UW System Associate Vice President of Information Security will require UWSA and the institutions to report their status with respect to implementing and complying with the systemwide information security policies and standards.

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 the resources.

All personnel covered by this program are obligated to report apparent violations. Any individual who suspects a violation of this program and it's supporting policies shall report it to their institution Information Security Officer or alternatively to the UW Administration Chief Information Security Officer. If the violation does not appear to be resolved in a timely manner, either the UW System CISO or AVP for Information Security shall be notified by the person observing the violation.

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 a 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 Exceptions

While deviation from this IS program is discouraged, an exception process exists that allows for certain scenarios which cannot be effectively addressed within the constraints of UW System's information security program and supporting policies and standards.

Any potential exceptions to the Information Security policies and associated standards should be evaluated based on the risk associated with the particular situation. This should include factors related to data classification, institutional objectives, regulatory and compliance matters, systems and processing criteria, and technology.

Requests for exceptions to any element of this program and its supporting policies and standards shall be submitted in writing by the Chancellor's designee for Information Technology environments to the Associate Vice President for the Office of Learning and Information Technology Services (UW System CIO). Upon agreement by the AVP, the request for exception shall be submitted in writing to the AVP for Information Security. In the case of exception to a

specific procedure, the compensating control process identified in the procedure shall be followed.

11.0 Legal or Regulatory Requirements

The UW System continuously endeavors to comply with the information security requirements and implications of any applicable laws and regulations. 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.

12.0 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.

12.1 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.

Under the guidance of the UW System Information Assurance Council, the following policies and procedures have been developed and approved:

- Information Security: Authentication [1030]
  - Information Security: Authentication Procedures [1030.A.]
- Information Security: Data Classification and Protection [1031]
  - Information Security: Data Classification Procedures [1031.A.]
  - Information Security: Data Protections Procedures [1031.B.]
- Information Security: Awareness [1032]
- Information Security: Incident Response [1033]
- Acceptable Use of Information Technology Resources [Regent Policy Document 25-3]

The two-year action plan accompanying the April 2018 version of this Information Security Program document calls for the UW System to review and update associated policies and standards to align with systemwide security goals. A list of proposed policies and standards can be found in appendix C.

12.2 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.

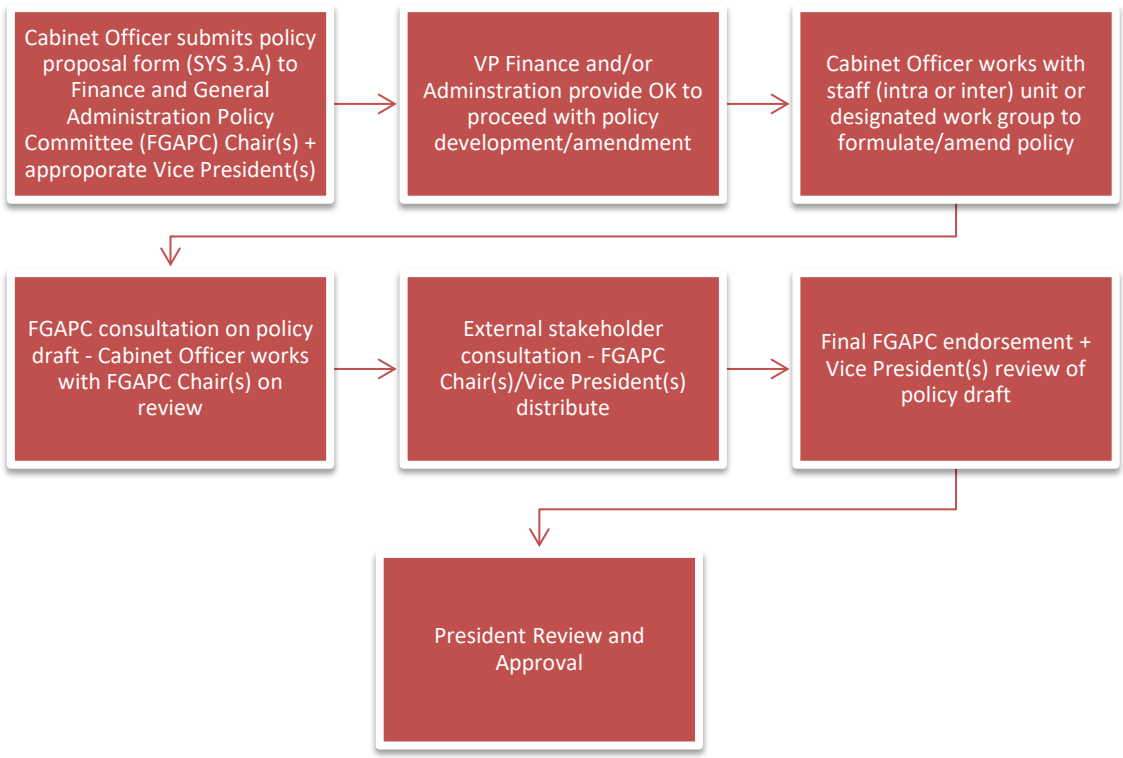

Figure 1: UW System Administrative Policy Development Process

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.

Regarding information security, the major effort for policy development and amendment is carried out by the UW System Information Assurance Council.

Appendix A: Glossary

Terms	Definition
Access Control List (ACL)	An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.
Access Modes	The concept of access modes is fundamental to access control. Common access modes, which can be used in both operating systems and applications, include read, write, execute, and delete. Other specialized access modes (found more often in applications) include create or search.
Address Space Layout Randomization (ASLR)	Address space layout randomization (ASLR) is a memory-protection process for operating systems (OSes) that guards against buffer-overflow attacks by randomizing the location where system executables are loaded into memory.
Advanced Encryption Standard (AES)	The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.
Asset Management	IT asset management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment.
Attack Vectors	An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.
Authentication	The process of verifying that someone who holds an account on an IT system is who they purport to be.
Authorization	Authorization is the function of specifying access rights/privileges to resources related to information security and computer security in general and to access control in particular.
Availability	Availability of information refers to ensuring that authorized parties are able to access the information when needed.

Bogon	A bogon is a bogus IP address from the bogon space, which is a set of IP addresses not yet officially assigned to any entity by the Internet Assigned Number Authority (IANA) or a regional Internet registration institute.
Bring Your Own Device (BYOD)	Bring your own device (BYOD)—also called bring your own technology (BYOT), bring your own phone (BYOP), and bring your own personal computer (BYOPC)—refers to the policy of permitting employees to bring personally owned devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.
Business Continuity Plan	Business continuity planning (or business continuity and resiliency planning) is the process of creating systems of prevention and recovery to deal with potential threats to a company.
C2 Domains	A command-and-control [C&C] server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.
Center for Internet Security (CIS)	The Center for Internet Security (CIS) is a nonprofit organization, formed in October 2000 whose mission is to "identify, develop, validate, promote, and sustain best practice solutions for cyber defense and build and lead communities to enable an environment of trust in cyberspace".
Cold Logs	Cold logs do not necessarily require immediate action but may provide value when summarized or analyzed later.
Communication Plan	A communication plan is a policy-driven approach to providing stakeholders with information. The plan formally defines who should be given specific information, when that information should be delivered and what communication channels will be used to deliver the information.
Compliance	Compliance is the act of adhering to, and demonstrating adherence to, external laws and regulations as well as corporate policies and procedures.
Computer Incident Response Team	A computer security incident response team (CSIRT) is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident.
Confidentiality	Confidentiality, in the context of computer systems, allows authorized users to access sensitive and protected data.

Containerization	Application containerization is an OS-level virtualization method used to deploy and run distributed applications without launching an entire virtual machine (VM) for each app. Multiple isolated applications or services run on a single host and access the same OS kernel.
Containment	Limiting the damage of the incident and isolating affected systems to prevent further damage.
Damage Assessment	Preliminary but fairly accurate onsite evaluation of damage or loss caused by an accident or natural event before filing a formal claim or disaster declaration. Damage assessment records the extent of damage, what can be replaced, restored, or salvaged, and time required for their execution.
Data Breach	A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
Data Custodian	A term describing a UW System employee that has been given formal responsibility for the security of the asset or the data hosted on the asset. It does not mean that the asset belongs to the owner in a legal sense.
Data Execution Prevention (DEP)	Data execution prevention (DEP) is a security feature within operating system that prevents applications from executing code from a non-executable memory location. DEP is a hardware and software enforced technology designed to secure against memory-based code exploits. It was first introduced in Windows XP Service Pack 2.
Data Loss Prevention	Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.
Data Reduction	Data reduction is the transformation of numerical or alphabetical digital information derived empirically or experimentally into a corrected, ordered, and simplified form.
Data Steward	An individual who has direct responsibility to ensure that a data set is classified appropriately. The data steward collaborates with institutional Security, Privacy and Data Officers.

Defense Information Systems Agency (DISA)	The Defense Information Systems Agency (DISA) is a U.S. Department of Defense (DoD) combat support agency composed of military, federal civilians, and contractors. DISA provides information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military services, the combatant commands, and any individual or system contributing to the defense of the United States.
Demilitarized Zone (DMZ)	In computer security, a DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. The purpose of a DMZ is to add an additional layer of security.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on TCP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network, so they can communicate with other IP networks.
Disaster Plan	A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster.
Domain Name System (DNS)	The domain name system (DNS) is the way that internet domain names are located and translated into internet protocol (IP) addresses.
Enhanced Mitigation Experience Toolkit (EMET)	Enhanced Mitigation Experience Toolkit (EMET) is a freeware security toolkit for Microsoft Windows, developed by Microsoft. It provides a unified interface to enable and fine-tune Windows security features.
Enterprise and Host Forensics	Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.
End of life Operating System	End-of-life (EOL) is a term used with respect to a product supplied to customers, indicating that the product is in the end of its useful life (from the vendor's point of view), and a vendor stops marketing, selling, or rework sustaining it. (The vendor may simply intend to limit or end support for the product.)
Eradication	Finding the root cause of the incident, removing affected systems from the production environment.

Extensible Authentication Protocol-Transport Layer Security (EAP/TLS)	Extensible Authentication Protocol (EAP) is used to pass the authentication information between the supplicant (the Wi-Fi workstation) and the authentication server (Microsoft IAS or other). EAP-TLS (Transport Layer Security) provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.
Federal Information Processing Standard (FIPS) 140-2	The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.
Full Packet Capture	Packet capture is a computer networking term for intercepting a data packet that is crossing or moving over a specific computer network.
Full-Disk Encryption (FDE)	Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume.
Host Based Scanning	Host based scanning refers to directly installing the scanner on the host to be scanned. This gives the scanner access to low-level data, such as specific services and configuration details of the host's operating system. It can therefore provide insight into risky user activities such as using easily guessed passwords or even no password.
Identity (user ID)	The identity is usually unique to an individual in order to support individual accountability, but it can also be a group identification or even anonymous.
Identity management	In enterprise IT, identity management is about establishing and managing the roles and access privileges of individual network users.
Indicators of Compromise (IOC)	Indicators of compromise (IOC) — in computer forensics is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion. Typical IOCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs or domain names of botnet command and control servers.
Integrity	Integrity of information refers to protecting information from being modified by unauthorized parties.

Intrusion Detection Systems (IDS)	An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.
Intrusion Prevention System (IPS)	An intrusion prevention system (IPS) is a system that monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.
IT Disaster	An IT disaster is an incident that causes disruption to IT systems, such as a server failure, security breach, or data loss.
Level of Assurance	A Level of Assurance, as defined by the by ISO/IEC 29115 Standard, describes the degree of confidence in the processes leading up to and including an authentication. It provides assurance that the entity claiming a particular identity, is the entity to which that identity was assigned.
Location	Access to specific system resources may be based upon the user's physical or logical location. Similarly, users can be restricted based upon network addresses.
Log Analysis	In computer log management and intelligence, log analysis (or system and network log analysis) is an art and science seeking to make sense out of computer-generated records (also called log or audit trail records).
Malware	Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software, [1] including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other intentionally harmful programs.
Master Image	In network virtualization, a golden image is an archetypal version of a cloned disk that can be used as a template for various kinds of virtual network hardware. Some refer to the golden image as a master image because multiple copies are used to provide a consistent process for using a disk image.
Maximum Allowed Outage Time	The Maximum Allowed Outage Time is the longest period of time a system or service can stop functioning without having a severe impact on the business.
Mobile Device Management (MDM)	Mobile device management (MDM) is a type of security software used by an IT department to monitor, manage and secure employees' mobile devices that are deployed across multiple mobile service providers and across multiple mobile operating systems being used in the organization.

Multi-Factor Authentication	Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
National Institute for Standards and Technology (NIST)	The National Institute of Standards and Technology (NIST) is a measurements standards laboratory, a non-regulatory agency working under the U.S. Department of Commerce.
NetFlow	NetFlow is a network protocol developed by Cisco for the collection and monitoring of network traffic flow data generated by NetFlow-enabled routers and switches.
Network Based Scanning	Network scanning refers to the use of a computer network to gather information regarding computing systems. Network scanning is mainly used for security assessment, system maintenance, and also for performing attacks by hackers.
Patch Management	Patch management is a strategy for managing patches or upgrades for software applications and technologies. A patch management plan can help a business or organization handle these changes efficiently.
Payment Card Information (PCI)	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.
Penetration Testing	Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.
Period of Criticality	The period of criticality is the duration after an emergency that is most critical to the state of the system.

Personally Identifiable Information (PII)	"PII is commonly defined as any data that could identify a specific individual. Information that can be considered PII includes, without limitation, the following: • An individual's first name and last name • Government-issued identification number • Social Security Number (SSN) • Driver's license number • Passport number • Credit card, debit card, Bank account, or other financial account number • Medical health information (physical or mental) • Personal Identification Code • Biometric and/or genetic data • Email names or addresses, and other electronic identification numbers • Geolocation data • Digital Signatures • Individual's log-in credentials, such as a username and password • Parent's legal surname prior to marriage • Consumer data (<13 years of age) • Racial or ethnic origin • Political, religious, or philosophical beliefs • Criminal record and civil offenses • Sexual preferences or practices • Social organization membership
Phishing	Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
Production	A production environment is where the real-time staging of programs that run an organization are executed, and includes the personnel, processes, data, hardware, and software needed to perform day-to-day operations.
Protected Health Information (PHI)	Protected health information (PHI) under the US law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.
Proxy	In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.

Ransomware	Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
Recovery	Permitting affected systems back into the production environment, ensuring no threat remains.
Recovery Time Objective (RTO)	Recovery time objective (RTO) is the targeted duration of time and a service level within which a process must be restored after a disruption to avoid consequences with a break in business continuity.
Recovery Point Objective (RPO)	Recovery point objective (RPO) is the maximum targeted period in which data might be lost from an IT service due to a major incident. The RPO gives systems designers a limit to work to.
Recovery Prioritization Score (RPS)	Recovery prioritization score (RPS) is a metric to help organizations prioritize resource to guide effective plans and realistic test scenarios.
Residual Risk	Residual risk is the threat that remains after all efforts to identify and eliminate risk have been made.
Reverse Engineering	Reverse engineering, in computer programming, is a technique used to analyze software in order to identify and understand the parts it is composed of.
Risk	Risk is the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.
Risk Appetite	Risk appetite can be defined as 'the amount and type of risk that an organization is willing to take in order to meet their strategic objectives.
Risk Exposure	Risk exposure is a quantified loss potential of business. Risk exposure is usually calculated by multiplying the probability of an incident occurring by its potential losses.
Risk Profile	A risk profile is an evaluation of an individual or organization's willingness to take risks, as well as the threats to which an organization is exposed.
Risk Tolerance	Risk tolerance “reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve”
Role	Access to information may be determined by the job assignment or function (i.e. the role) of the user who is seeking access. Roles should be defined based on a thorough analysis of how the organization operates, including input from a wide spectrum of users.

Role-based Access	Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file.
SDLC	The software development life cycle (SDLC) is a framework defining tasks performed at each step in the software development process. SDLC is a structure followed by a development team within the software organization. It consists of a detailed plan describing how to develop, maintain and replace specific software.
Security Controls	Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.
Security Information and Event Management (SIEM)	Security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.
Sender Policy Framework (SPF)	Sender Policy Framework (SPF) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators.
Service Constraints	Service constraints refer to those restrictions that depend upon the parameters that may arise during use of the application or that are pre-established by the resource owner/manager.
Shoulder Surfing	In computer security, shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder.
Social Engineering	Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.
Software Quality Assurance (QA)	Software quality assurance (SQA) is a process that ensures that developed software meets and complies with defined or standardized quality specifications.
Spear phishing	Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons.

Staging	A staging server is a type of server that is used to test a software, website or service in a production-similar environment before being set live.
Standards	A specific set of minimum characteristics or requirements, usually measurable, that must be met in order to comply.
Subject Matter Expert (SME)	A subject matter expert (SME) is a person who is an authority in a particular area or topic.
Subnet	A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.
Threat and Vulnerability Management (TVM)	Vulnerability management is the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities", particularly in software.
Threat Intelligence	Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.
Time	Time-of-day and day-of-week/month restrictions are another type of limitation on access.
Transaction	Systems handling transactions may limit access based on transactions. For example, system might grant access to an account for only the duration of a transaction. In an account inquiry, a caller might enter an account number and PIN. A service representative would then be given read access to that account. When the transaction is completed, the access authorization is terminated. With this approach, users (service representatives, in this example) are given access only to the account involved in the transaction.
Transmission Control Protocol (TCP)	Transmission control protocol (TCP) is a network communication protocol designed to send data packets over the Internet.
User Acceptance Testing (UAT)	User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications.
Virtual Local Area Network (VLAN)	A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

Virtual Private Network (VPN)	A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. VPN technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources.
Virtualization	In computing, virtualization means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments.
Vulnerability Scanning	Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.
Warm Logs	Warm logs are logs that are clear, actionable and require immediate attention.
Web Application Firewall (WAF)	A web application firewall (WAF) is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.
Wi-Fi Protected Access 2 (WPA2)	Short for Wi-Fi Protected Access 2, WPA2 is the security method added to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks.
Zero Day Attacks	A zero-day attack is an attack that exploits a previously unknown vulnerability.

Appendix B: UW System President Memo of 4 April 2018

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

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.

Appendix C: UW System Proposed Information Security Policies

The following is a list of proposed policies and minimum standards that are incorporated into the UW System policy development process in accordance with the prioritized actions outlined in the accompanying two-year work plan.

Proposed Policies:

- Information Security: Asset Management [1035]
- Information Security: Endpoint Protection [1036]
- Information Security: IT Disaster Recovery [1037]
- Information Security: Network Protection [1038]
- Information Security: Risk Management [1039]
- Information Security: Personal Data Privacy [1040]
- Information Security: Secure Software Development [1041]
- Information Security: Security Monitoring [1042]
- Information Security: Threat and Vulnerability Management [1043]

Proposed Standards:

- Information Security: Asset Management Standards [1035.A.]
- Information Security: Data Protection Standards [replaces 1031.B.]
- Information Security: Endpoint Protection Standards [1036.A.]
- Information Security: Incident Response Standards [1033.A.]
- Information Security: Identity and Access Management Standards [replaces 1030.A.]
- Information Security: Information Technology Disaster Recovery Standards [1037.A.]
- Information Security: Network Protection Standards [1038.A.]
- Information Security: Risk Management Standards [1039.A.]
- Information Security: Security Awareness and Training Standards [1032.A.]
- Information Security: Secure Software Development Standards [1041.A.]
- Information Security: Security Monitoring Standards [1042.A.]
- Information Security: Threat and Vulnerability Management Standards [1043.A.]