WAYNE STATE
UNIVERSITY
Computing & Information Technology

Wayne State University Information Security Program Charter

Purpose

This document describes the Wayne State University Information Security Program. This program is a set of policies, procedures and responsibilities for the protection of institutional data. The Information Security Program is intended to ensure the confidentiality of university records and related computing resources, protect against anticipated threats and hazards to the integrity of university data and prevent unauthorized access to information or computer resources associated with protected university data.

Data Covered by the Information Security Program

Covered Data includes any Wayne State University data as defined by the Wayne State Data Governance committee.

Information Security Program Overview

This Information Security Program is based the best practices published by the National Institute of Standards and Technologies (NIST) covering the following key elements:

1. Designating an employee or office responsible for coordinating the program
2. Conducting risk assessments to identify reasonably foreseeable security and privacy risks
3. Ensuring that safeguards are employed to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored
4. Overseeing third-party security risks
5. Maintain and adjusting the Information Security Program as needed

The Information Security Program at Wayne State University follows the centralized and distributed model of IT service delivery. The centralized elements of the program consist of a set of common controls that include such functions as security policy implementation, awareness and training, incident response, and security infrastructure. Distributed elements of the program include use of common controls, controls delivered as part of a C&IT service, and any controls or safeguards necessary to secure the special IT needs of each school, college or division. . Leadership for the centralized elements and coordination of the distributed elements of the program are the responsibility of the Program Officer.

Information Security Program Elements

Security Responsibility and Authority.

The Information Security Program is governed by the Information Security and Risk Oversight Group as created by the Information Security Oversight Committee. The oversight group is responsible for providing strategic oversight of the Information Security Program and maintaining the Information Security Program Charter.

The Sr. Director of Information Security under the division of Computing & Information Technology is designated as the Chief Information Security Officer ("Program Officer") responsible for coordinating and overseeing the Information Security Program. The Program Officer may designate other representatives of the University to oversee and coordinate portions of the program. Any questions regarding the implementation of this program or the interpretation of this document should be directed to the Program Officer or her or his designees.

The Program Officer will consult with academic and administrative leadership to create a plan that aligns with the University's strategic vision and values. At a minimum:

- The Program Officer will establish and provide leadership for the Information Security Office that is tasked with execution of the Information Security Plan.
- The Program Officer will work closely with the data governance committee, to ensure all areas with covered information are included within the scope of this Information Security Program.
- The Program Officer will consult with responsible offices of each school, college and division to identify the security risks and specific needs of each units and areas of the University with access to covered data.
- The Program Officer will periodically conduct security assessments of units to test safeguards and ensure compliance.
- The Program Officer will create and maintain an Incident Response Policy for addressing information security incidents.
- The Program Officer will, in consultation with other University offices, verify that existing policies, standards and guidelines that provide for the security of covered data are reviewed and adequate.
- The Program Officer will make recommendations for revisions to policy, or the development of new policy, as appropriate.
- The Program Officer will work with responsible parties to ensure that the departmental training and education plans are developed and delivered for all employees with access to covered data.

The Program Officer may require units with substantial access to covered data to further develop and implement comprehensive security plans specific to those units and to provide copies of the plan documents.

The Program Officer may designate, as appropriate, responsible parties in each area or unit to carry out activities necessary to implement this Information Security Program.

Risk Assessment. The Program Officer shall in conjunction with the Office of Internal Audit conduct periodic risk assessments for departments that manage and/or process sensitive or regulated information. These risk assessments will identify and assess both internal and external risks to the confidentiality, integrity and availability of covered data and IT devices that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of the information. Sensitive information includes, but is not limited to, nonpublic customer information as defined by the Wayne State Data Governance Committee and other categories of information protected by law and/or University policy, and information relating to the IT devices that process such information.

Risk assessments will include, but are not limited to, assessments of access, handling and storage procedures for both electronic and non-electronic information, network and system assessments, and appropriate incident response and reporting.

Develop Safeguards to Mitigate Identified Risks. To address and mitigate risks identified in the assessment effort of this program the Program Officer will lead the development of physical and IT safeguards and security operations to appropriately address and minimize the effects of security incidents. The broad areas in which this is achieved are further described below.

> Secure Infrastructure. The Information Security Program will provide fora common secure infrastructure for information systems and their respective data to operate in a safe and trusted manner. A secure infrastructure protects against the inadvertent disclosure, alteration, or destruction of data while it is being transmitted, stored, or processed.
>
> Secure Applications. The Information Security Program will ensure applications which process and handle information critical to the University must be procured, developed, tested and implemented in a secure and consistent environment. Application security protects against disclosure or alteration of data during processing.
>
> Identity and Access Management. The Information Security Program will provide a mechanism for managing the lifecycle of accounts used for accessing general computing resources for staff, faculty, students, alumni and other affiliates of Wayne State during the duration of their association with the University. This mechanism will provide for a process to grant and remove access to enterprise applications that contain confidential and sensitive information following the principle of least privilege
>
> Principle of least privilege is defined as the minimum system access and system resources necessary to perform a business process.
>
> Security Education. The Information Security Program will support education of University constituents to ensure that published practices and guidelines are followed and understood effectively. The University will provide security education resources and analysis to assist university constituents and the community secure their personal and university-related systems and data.
>
> Incident Detection and Response. The Information Security Program will create a process to provide timely and accurate identification of IT incidents, perform comprehensive analysis of exposure or loss, and coordinate remediation commiserate with exposed risk.

Program Governance. The Information Security Program will establish a governance process to provide oversight, direction, and accountability for the Information Security Program. By following common frameworks and providing constructive feedback, metrics, and actionable items to the Information Security Program, continual improvement will be achieved.

Risk Management. The Information Security Program will establish a mechanism for tracking information security risk identified through the risk assessment process to ensure timely remediation of security risk. This mechanism will provide for processing and tracking exceptions to Information Security Policy, Standards and Guidelines along with establishing an approval process commensurate with the level of identified risk.

Security Oversight of University Service Providers. The Program Officer shall coordinate with those responsible for the third party service procurement activities (Wayne State Computing & Information Technology and other affected divisions or departments) to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for proper information handling and protection. In addition, the Program Officer will work with Office of General Counsel, Wayne State Computing & Information Technology, and any other affected units or departments to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the Office of General Counsel. These standards shall apply to all contracts entered into with such third party service providers.

Adjustments to the Information Security Program. The Program Officer is responsible for evaluating and recommending adjustments to the Wayne State Information Security Program based on the risk identification and assessment activities undertaken pursuant to this program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on this program.

Exceptions to the Program

Exceptions or waivers to this Program or its subsequent practices, procedures or standards must be authorized by the Program Officer. Exceptions or waivers to any practices, controls, or standards will be properly documented and reviewed on a periodic basis.

Program Enforcement

The University reserves the right to monitor electronic systems and networks, perform periodic audits, and take appropriate steps to ensure the security of its information and compliance with this program. Violations of this Program may result in the loss or restricted use of information systems or services and disciplinary action per the advisement of Human Resources, Labor Relations, and the Office of the General Counsel.

Privacy

While there are many areas of overlap between security and privacy the information security program is not designed to address privacy concerns of covered data, which is covered by the University Privacy

Policy. However, the information security office will take all measures possible to address proper handling of data that is required to secure the University and will only use such data for the intended purposes outlined in this charter.

Appendix A – Information Security Office Service Offerings

This appendix is intended to be a non-exhaustive list of services provided by the Information Security Office (ISO). The below matrix describes how services are delivered for centralized IT services, or common controls, across the University and how services may be used by each school, college or division (S/C/D) as part of distributed IT service delivery. Additional details, including how to request services, can be found in the University IT Service Management System or the knowledge base at tech.wayne.edu.

Service Offering	Centralized	Distributed
Firewall Management	The ISO manages and maintains two core sets of firewalls as part of the common University Network. The border firewall protect the University Network from unauthorized access. The border firewall contains mechanisms to protect against malware and network intrusions. The production firewall protects assets in the C&IT Data Center from unauthorized access from both external and internal networks.	Some S/C/D may require an additional level of security or have special compliance requirements that require firewalls in other areas of the campus network. The ISO offers a service to provide, manage and maintain firewalls if additional protection is needed.
VPN Management	The ISO manages and maintains a VPN appliance for establishing secure connectivity to external affiliates of the University. These are commonly referred to as site-to-site VPNs. The ISO will setup and maintain site-to-site VPN connections as long as the remote affiliate is compatible with the University appliance.	Some S/C/D may have additional requirements that require specialized devices for VPN connectivity. The ISO will help support connectivity of those VPN connections through the campus network but does not manage any VPN endpoints outside of the common VPN appliance. It is recommended that any S/C/D that needs these VPN services contact the ISO prior to deployment.

Secure Remote Access	The ISO manages and maintains a remote access solution for providing secure connectivity to University IT resources from outside the campus network. This is commonly referred to as client VPN. This service is provided for staff, faculty, and affiliates. (Guest and students may be allowed by exception).	It is recommended that all S/C/D use the central remote access solution. If there are special requirements for remote access please contact the ISO to review.
Certificate Management	The ISO provides a service to issue signed SSL/TLS server certificates for use in accordance with University guidelines. Signed certificates may also be issued for other needs such as code signing or esignatures as exceptions.	Certificates used for externally facing services for the wayne.edu domain or subdomains must be issued by the ISO. Signed certificates for nonwayne.edu domains or other special needs may be acquired outside of the ISO service offering but must follow University guidelines.
Identity and Access Management	The ISO automatically provisions and deprovisions access for any person associated with the University based on their role and duration they are affiliated with the University for common computing resources.	This service is University wide for all common resources and not applicable to specialized needs of S/C/D. However, S/C/D are encouraged to use Wayne Access IDs and Single Sign On system for controlling access to specialized applications.
Enterprise System Access	The ISO is responsible for provisioning and deprovisions access to core enterprise applications such as Banner, STARS, Cognos and ODS. Access is granted based on request from BAOs to pre-defined business roles following least privilege methodology.	This only applies to enterprise systems and not applicable S/C/D.

Service and Group Accounts	The ISO creates service accounts, application IDs, security profiles and other group accounts for use in core enterprise applications.	This only applies to enterprise systems and not applicable S/C/D.
Privileged Identity Management	The ISO provides a centralized tool for securely storing and sharing accounts and password related to administrative activities for all C&IT staff.	This service is current only available to C&IT. S/C/D may contact the ISO to discuss special needs.
Multi-Factor Authentication	The ISO provides two-factor authentication for employee self-service applications that contain sensitive data such as time sheets and direct deposit. Two-Factor authentication is provided for administrative access to C&IT managed systems.	Two-factor authentication may be available to other applications that use the Wayne Single Sign On service. S/C/D should contact the ISO directly to discuss options if two-factor is required.
Vulnerability Management	The ISO provides vulnerability scanning and reporting services for the University network and attached infrastructure. Reports are delivered to the appropriate remediation teams on a monthly basis. The ISO offers authenticated scans for devices connected to the WSU domain or have the appropriate accounts configured.	S/C/D that are responsible for vulnerability remediation have been identified and receive monthly reports. S/C/D may contact the ISO to discuss other special needs.
Infrastructure Security Testing	The ISO performs periodic external infrastructure testing for enterprise applications and the University network. Testing is performed based on identified risk or during implementation of new infrastructure.	The ISO has partnered with an external organization for testing. S/C/D may use the same partner for special testing through the ISO. If other organizations are used they must be approved by the ISO.

Application Code Review	The ISO performs periodic code review of C&IT developed applications to ensure compliance with University application development standards.	This service is only offered for C&IT developed applications due to the broad scope of application development requirements outside of C&IT. S/C/D may contact the ISO to discuss options for specific needs.
Application Security Testing	The ISO performs periodic external application testing for enterprise applications. Testing is performed based on identified risk or during implementation of new applications.	The ISO has partnered with an external organization for testing. S/C/D may use the same partner for special testing through the ISO. If other organizations are used they must be approved by the ISO.
Security Event Logging and Monitoring	The ISO provides a SIEM tool for collecting system logs from common infrastructure such as Active Directory, LDAP, servers, databases DNS, wireless controllers, firewalls and other security tools. These logs are used for identifying and responding to security incidents and are not retained for long term storage.	S/C/D may choose to send logs to the ISO SIEM but is not mandatory unless required by ISO to support a security investigation. Other C&IT services may include collection and monitoring of logs. If an S/C/D is unsure of what is collected or has special needs they should contact the ISO to discuss options.
Security Incident Response	The ISO creates, maintains and performs periodic testing of the University Security Incident Response Plan (SIRP). The ISO will investigate any potential security incident to determine if the SIRP should be enacted. If the SIRP is enacted the ISO will act as primary coordinator throughout the incident lifecycle.	The ISRP covers the entire University. All suspected security incidents should be reported by S/C/D to the ISO. The ISO encourages each S/C/D to maintain documentation for responding to security incidents as required by the roles and responsibilities outlined in the ISRP.

Third-Party Security Review	The ISO performs third-party security review as part of C&IT procurement services or as required as part of a security incident investigation.	C&IT procurement services are offered to all S/C/D. The C&IT procurement office should be contacted for details.
Security Governance	The ISO identifies, creates, and maintains policies, standards and guidelines related to Information Security. This includes reviewing and update the Information Security Plan.	Information Security policies, standards and guidelines are expected to followed by all S/C/D. If there is a specific need for an information security policy, standard or guideline S/C/D may contact the ISO to discuss options.
Information Security Consulting	The ISO provides general consulting services for C&IT projects or to supplement existing ISO service offerings	ISO consulting is generally available for any S/C/D contact the ISO directly to discuss details.
Information Security Awareness and Training	The ISO provides a suite of tools for general security awareness and training to staff, faculty and students using various forms of media including formal training for users of enterprise applications.	While the ISO focuses on widely publishing general security knowledge commonly requested specialized training is also available for smaller audiences. S/C/D that have specialized training needs should contact the ISO to discuss options.

Last updated: Feb. 28, 2020