

Position Description

University Information Security Officer – Miami University

Basic Function and Responsibility: The University Information Security Officer (ISO) position is responsible for development, implementation and management of an information security management program for the entire university. The incumbent will research and evaluate procedural and technical solutions that can be applied on the campus networks, manage the University's response to security incidents and maintain configuration control of security devices and software applied to centralized network and systems supporting the University.

Essential Duties and Responsibilities

Management

The ISO will maintain a knowledge of University network architecture and both central and departmental application servers in order to better understand the risk of system exposure, recommend realistic preventive measures, respond to information security incidents, and plan for system upgrades or introduction of new systems to the network environment.

The ISO will report for scheduled work in a dependable and timely fashion in order to be available to systems administration and Network Operations Center personnel, IT Services management or University customers. The person in this position is expected to provide after-hours on-call support as necessary to respond to information security incidents in order to return affected systems to production use in a timely manner.

This person will assign tasks, instruct, or give instructions to student assistants, part-time workers, matrixed staff and security staff direct reports in order to ensure that business requirements are met.

The ISO must respond to telephone calls, voice messages, pages and electronic mail within one day of receipt and maintain his or her activity calendar in the Meeting Maker system and provide read access as a minimum to the Vice President for Information Technology and Administrative Assistant in order to allow efficient use of time for necessary meetings and discussions.

On a daily basis, the ISO will review Miami's Remedy trouble tickets assigned to Security. Based upon this review, this person will use appropriate management techniques to resolve reported problems and requirements in a timely and efficient manner in order to resolve customer problems.

The ISO will comply with IT Services and Miami University developed procedures for submission of purchase requisitions, verification of fund expenditures and receipt of purchased items in order to ensure proper expenditure of funds and payment for materials actually received.

The ISO is expected to develop reports as necessary to keep IT Services management apprised of information security threats and active attacks, incident response activities and planned equipment or software changes that could impact system and network performance and availability in order to minimize the impact on production system users. The ISO is responsible for implementing an effective University network and computing asset protection mechanism to ensure stable and continuous operation of the University's mission-critical systems and applications.

This person will be expected to define and become actively engaged in information security tasks in projects involving IT Services or being managed by IT Services. As necessary, he or she will update appropriate time and status information of these tasks using MS Project and Project Central. The ISO serves as the point of contact within the office of the Vice President for Information Technology for security review of all new systems and platforms intended to be connected to the central network in order to ensure highest level of protection appropriate to use is included in purchasing and implementation planning.

The ISO is also charged with responsibility of assessing, reporting and assisting in the remediation of IT security vulnerabilities for non-IT Services managed systems and applications that are part of Miami University's purview. The ISO is expected to work positively and cooperatively with the University's Internal Audit staff, external auditors, EDP auditors, or other security-related contractors to address University information security issues. Also, the ISO will cooperate in a timely fashion with the University's legal affairs office, FERPA compliance officer, and others within the University involved in protection of privacy of information. The ISO will recommend to the Vice President for Information Technology, and implement as approved, the appropriate information security advisory groups, working committees and task forces to address University information security issues and procedures.

The ISO will attend established IT Services status updates and staff meetings in order to obtain and impart information on current and planned activity and items of concern to network operations center personnel.

The ISO will develop annual budget recommendations for training and capital expenses in compliance with the University's IT Strategic Plan in order that the ISO, IT Services staff and the broader University community remain proficient in necessary skills and are knowledgeable on applicable information security technology.

This person will develop continuing relationships with security product vendors and consultants and recommend as appropriate partnerships that would benefit Miami University.

The ISO will serve as the IT Services representative to designated University committees in order to provide technical advice and professional consultation on security issues, policies and procurements being considered.

Information Security Operations

The ISO will coordinate on a continuous basis with appropriate management to schedule and review periodic audits of network and system activity.

This person will also coordinate directly with University representatives to develop a Security Awareness Program and an Incident Response capability.

The ISO will coordinate with the Network Operations Center management and Support Center management on procedures for technician notification and currency of notification rosters. Additionally, he/ or she will develop with the Network Operations Center management, and IT Services management team for systems those checklists for use by any involved personnel to respond to information security incidents.

Configuration Control

The ISO is responsible for maintaining and updating the configuration files for information security appliances, software and equipment.

Also, he or she must coordinate with management the necessary access to equipment and systems necessary for security auditing, monitoring and incident response.

Training/Staff Development

The ISO is expected to identify job related training requirements and, within budgetary constraints, accomplish that training through an appropriate method. This should be communicated by the development of a written information security training and development plan.

The ISO is expected to participate on external university information security committees and the EDUCAUSE System Security Task Force as opportunities arise, as well as mentor other Ohio institutions or agencies through the delivery of security presentations and seminars. The ISO may conduct network assessments of other institutions under contractual agreements and attend EDUCAUSE conferences and other relevant university information security gatherings. The ISO is expected to ensure that both the ISO and the information security staff maintain an aggressive continuing education program to maintain currency in their field.

The ISO and his/her staff should document the information security-related skill proficiency of network, systems and network operations center employees and coordinate with appropriate managers to document as training may be identified and accomplished.

This person will assist in the creation and revision of job descriptions and tasks related to information security for employees in IT Services and other departments to identify skills

required to perform the tasks associated with each job and expected outcome of performance.

Educational Requirements

Bachelor's degree in information systems, computer science or some related discipline, or an equivalent number of years experience in an information systems or information security role.

Technical Knowledge and Skills

Minimum CISSP certification is required. Additional certifications are desirable.

Demonstrated understanding of supported system architectures and evolving technology

Demonstrated ability to perform ISO functions in a university, or similarly complex networking environment

Ability to develop and defend technical recommendations and budgetary plans

Ability to define and negotiate technical support contracts

Proficiency in MSOffice Suite, any e-mail application and MSProject/Project Central

Proficiency with Red Siren intrusion detection monitoring services, or similar services provided by other vendors

Additional skills in performing related information security functions are desirable.

Effectiveness Skills/Interactive Skills

The ISO should be able to:

Independently contribute ideas and process improvements and look for creative solutions and better ways of doing things, in order to meet goals of continuous improvement

Identify, analyze, and address problems in order to resolve issues whenever possible in a way that minimizes the negative impact on the organization

Communicate clearly and effectively about information security issues, while not creating the perception of exaggerated or unnecessary urgency. This communication style must be effective across a wide spectrum of individuals having varying degrees of technical understanding.

Understand the context of a university environment and how this differs from that of the private sector, corporate environment. This would include an appreciation of how security, privacy, academic freedom, intellectual property, open systems and academic enterprise networks fit into the university context.

Make appropriate, timely, and effective decisions, in order to support the work of the University, its divisions and departments

Adapt to new work situations, people, ideas, procedures, and organization structures, in order to accommodate a constantly evolving work environment. Exhibit willingness to learn new methods, be trained, provide training, and make job improvements. Demonstrate personal confidence about knowledge of the duties required to perform this job, as well as willingness to openly and effectively share that knowledge with others.

Build successful relationships with customers, co-workers, and administrators. Communicate and work effectively as a team member, in order to maximize the effectiveness of the work group

Demonstrate courtesy and consideration of others. Demonstrate a consistent willingness to do more than one's "fair share," and go beyond the call of duty in support of co-workers and customers

Exhibit good listening skills and demonstrate patience with others

Exhibit willingness to accept differences among individuals, be open-minded, and be willing to hear and accept others' suggestions.

Follow through on responsibilities and commitments in a timely fashion, and complete projects and other commitments when promised

Exhibit maturity, reliability, composure, and stability under pressure as required for handling on-the-job challenges. Be able to give and take constructive criticism well. Be gracious and slow to anger.

While at work, recognize that work is a priority and not let personal matters interfere with one's work obligations.

Demonstrate personal integrity and honesty.

Work successfully with diverse others and uphold the University's commitment to equal employment opportunity and affirmative action, in order to help the organization realize its commitment to excellence through diversity.