

UW Chief Information Security Officer

Responsibilities

The chief information security officer (CISO) is responsible for UW security policy and the coordination of information security efforts across the university. Working with UW senior management, the C&C strategic security manager, and the UW Medicine IT Services chief information officer, the CISO coordinates the process to build a university-wide security strategy and vision. The CISO oversees the creation and maintenance of UW information security policy, leads security risk assessment efforts, and owns the university awareness and training program. He or she also advises and collaborates with UW units on chain of trust agreements, business continuity and disaster recovery plans, and audit and governmental compliance practices.

In general, the CISO is charged with the responsibility for building a security-conscious culture for the University of Washington.

Duties

- Identify key security program elements and determine which UW departments or offices must be involved in building a comprehensive security program
- Lead the ongoing work of the UW Privacy Assurance and Systems Security (PASS) Council, whose oversight responsibilities include:
 - Developing, publishing, and maintaining comprehensive university-wide information privacy and security strategy, plans, policy, procedures, and guidelines
 - Acting as ombudsman for disputes, requests for exceptions, and complaints regarding university-wide information systems security policy, practices, and related issues
 - Acting as the primary control point during serious security incidents
 - Advising the university administration on risk issues that are related to security and recommending actions in support of the university's wider risk management programs
- Manage the development, implementation, and maintenance of UW security policy, standards, and guidelines
- Work with UW Internal Audit to ensure that departments consider information security risks in both ongoing and planned operations
- Keep university senior management informed about security-related issues and activities affecting the organization
- Understand potential threats, vulnerabilities, and control techniques and communicate this information to departmental system administrators
- Assist UW units as necessary to investigate security breaches and pursue associated disciplinary and legal matters

- Maintain relationships with local, state, and federal law enforcement and other related government agencies
- Work with Internal Audit, the Washington State Information Services Board, and outside consultants as appropriate on required security audits
- Direct the development and enforcement of information security and privacy policies in compliance with federal and state regulations and standards
- Develop a security awareness and training program
- Consult with UW departments on information security
- Work with C&C and Purchasing to create selection criteria for vendor products, tools, and services related to security
- Monitor and report on UW security activities

Reporting Relationships

The CISO will report directly to [a senior UW executive]. The CISO will work closely with the UW Medicine IT Services chief information officer and with the C&C strategic security manager. He or she will work with UW departments to coordinate security activities.

Qualifications

- Must be an intelligent, articulate, and persuasive leader who can serve as an effective member of the senior management team and communicate security-related concepts to a broad range of technical and non-technical staff
- Should have experience with business continuity planning, auditing, and risk management, as well as contract and vendor negotiation
- BA or BS in Computer Science, Information Management, or related field; Masters or PhD a plus
- Eight to ten years of progressive experience in computing and security, including experience with Internet technology and security issues
- Ability to work and effectively prioritize in a highly dynamic work environment
- Experience with disaster recovery planning and testing, auditing, risk analysis, business resumption planning, and contingency planning