Colleges of the Fenway

# Information Security Officer

Colleges of the Fenway (COF) is a collaborative effort of six neighboring Boston-based colleges in the Longwood Medical and Academic area. This collaboration was created to add value to student academic and social life while seeking innovative methods of investing in new services and containing the costs of higher education.

The **Information Security Officer** (ISO) is a position shared between Massachusetts College of Art and Design (MassArt) and Wentworth Institute of Technology (WIT), reporting jointly to their respective CIOs and to the assigned COF supervisor. At each institution, the ISO is responsible for establishing and maintaining information security management programs which meet business requirements, compliance and regulatory requirements and align with each institution's risk posture. The ISO will work with executive management at each institution to determine acceptable levels of risk for each organization, and will collaborate with functional areas, business units, academic departments and programs, to develop, implement, and monitor programs that incorporate information security best practices and industry standards.

The ISO is a thought leader, a consensus builder, and an integrator of people and processes. While the ISO is the leader of the security program, the ISO must also be able to balance multiple sets of requirements, and facilitate coordination and collaboration with teams at both institutions, while maintaining objectivity and a strong understanding that security is just one of each institution's activities.

## Primary Tasks and Areas of Responsibility

- Develop, implement and monitor a strategic, comprehensive enterprise information security and IT risk management program to ensure that the integrity, confidentiality and availability of institutional information and data is maintained consistent with business and academic processes, and best practices and standards.
- Facilitate information security governance through the implementation of governance programs, including the formation of information security steering committees or advisory boards.
- Develop, publish and maintain information security policies, standards and guidelines. Build consensus with the support of campus leadership for the approval, training, and dissemination of security policies and practices.
- Create, communicate and implement a process for technology risk management. This includes vendor risk management, the assessment and treatment for risks that may result from partners, consultants and other service providers, assessment of compliance and regulatory requirements, and identification of mitigation strategies and tactics.
- Supervise the Security Analyst at WIT.
- Develop and manage information security budget at WIT.
- Develop, implement, and monitor information security awareness training programs for all employees, contractors and approved system users.
- Work with stakeholders and functional areas at MassArt and WIT to facilitate IT risk assessment and risk management processes, identifying acceptable levels of residual risk.

MASSART MASSACHUSETTS COLLEGE OF ART AND DESIGN

WENTWORTH Institute of Technology

- Provide regular reporting on the current status of the information security program to enterprise risk teams and senior leaders and the board level audit team (WIT) as part of a strategic enterprise risk management program.
- Create or maintain a framework for roles and responsibilities with regard to information ownership, classification, accountability and protection.
- Provide strategic risk guidance for IT projects, including the evaluation and recommendation of technical controls.
- Liaise with various teams on each campus to ensure alignment between the security controls and the functional areas (e.g. enterprise IT architecture, finance, legal, HR).
- Coordinate information security and risk management projects with resources from the IT organization and business unit teams at each institution, in conjunction with the respective CIOs. Evaluate risk for all third party integrated systems.
- Ensure that security programs are in compliance with relevant laws, regulations and policies to minimize or eliminate risk and audit findings.
- Define and facilitate the information security risk assessment process, including the reporting and oversight of mitigation efforts to address negative findings.
- Manage security incidents and events to protect corporate IT assets, including intellectual property, regulated data and the colleges' reputations and direct the efforts of the security analyst at Wentworth.
- Monitor the external threat environment for emerging threats, and advise relevant stakeholders on the appropriate courses of action.
- Liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure that the organization maintains a strong security posture.
- Develop and oversee an effective disaster recovery plan and standards. Coordinate the development of implementation plans and procedures to ensure that mission-critical services are recovered in the event of a security event. Provide direction, support and in-house consulting in these areas.
- Once the programs are in place and in good working order, (likely in year 3) facilitate a metrics and reporting framework to measure the efficiency and effectiveness of the program, facilitate appropriate resource allocation, and increase the maturity of the security.
- Understand and interact with related disciplines through committees to ensure the consistent application of policies and standards across all technology projects, systems and services, including, but not limited to, privacy, risk management, compliance and business continuity management.
- Perform additional duties and fulfill responsibilities as required.

**Background and Experience**

- Bachelor's degree required in business administration or a technology-related field preferred.
- Minimum of five years of experience in a combination of risk management, information security and IT jobs. At least four must be in a leadership role. Employment history must demonstrate increasing levels of responsibility.
- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate security and risk-related concepts to technical and nontechnical audiences.

- Proven track record and experience in developing information security policies and procedures, as well as successfully executing programs that meet the objectives of excellence in a dynamic environment.
- Poise and ability to act calmly and competently in high-pressure, high-stress situations.
- Must be a critical thinker, with strong problem-solving skills.
- Knowledge and understanding of relevant legal and regulatory requirements, such as *Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry/Data Security Standard, Family Educational Rights Privacy Act (FERPA) and Sarbanes-Oxley Act (SOX).*
- Exhibit excellent analytical skills, the ability to manage multiple projects under strict timelines, as well as the ability to work well in a demanding, dynamic environment and meet overall objectives.
- Project management skills: financial/budget management, scheduling and resource management.
- Ability to partner with senior leadership to motivate and lead cross-functional, interdisciplinary teams to achieve tactical and strategic goals.
- Professional security management certification, such as a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) or other similar credentials, is desired.
- Knowledge of common information technology and information security frameworks such as ISO/IEC 27001, ITIL, COBIT and ones from NIST.
- Experience with contract and vendor negotiations.
- High level of personal integrity, as well as the ability to professionally handle confidential matters, and show an appropriate level of judgment and maturity.
- High degree of initiative, dependability and ability to work with little supervision.

**Qualified and Interested?**
Submit your resume and cover letter via https://theapplicantmanager.com/jobs?pos=M3213.
Principals only please. Relocation assistance not available.