Executive Director, Chief Information Security Officer

Chicago, IL

Summary

The Chief Information Security Officer is responsible for the development, delivery and administration of an organizational information security program and corresponding functions that include strategy, tactics, standards and systems. This position requires a high level of knowledge in the areas of risk assessment, network and system security, security implementation, and changing the culture of the institution through training and education. The position reports to the Senior Vice President, Chief Information Officer, but recognizing the enterprise-wide nature of the responsibility, the CISO will frequently be involved with policy development and systems security analysis throughout UCM. The CISO will lead the continued implementation and optimization of UCM's security strategies and capabilities.

Responsibilities:

- Develop, implement, and maintain an organizational information security program, developing an annually revised corresponding strategic plan and goals.
- Direct the strategies of the UCM IT identity and access management team, including the deployment of identity and access management platforms and solutions across the health system.
- Collaborate with peer stakeholders to enhance and strengthen an IT security risk management program which identifies and reduces risks on an ongoing basis by, aligning and prioritizing information security activities to mitigate business risk priorities. Reports quarterly to the Board of Trustees Audit Committee on the UCM Enterprise Risk Management progress.
- Coordinate and support external and internal audits and assessments of UMC IT security, including reviews performed by UCM's Internal and External Auditors, and collaborate with UMC IT leaders responsible for disaster recovery and continuity planning to ensure security requirements are accounted for.
- Ensure organizational compliance in accordance with information security policies, standards, procedures; responsible for the exception process, authorizes and documents all exceptions, and maintains a repository of all exceptions.
- Collaborate with the UCM IT operational units & leaders to define the appropriate information assurance technical measures required to secure the UCM network, endpoints, applications, and data.
- Ensure that a visible and effective Incident Response Policy and Procedure is in effect for timely enforcement, tracking and reporting.
- Maintain knowledge of security-related regulatory requirements and laws (e.g., HIPAA, HITECH, PCI, 405(d)), standards (NIST, COBIT, ISO etc.) affecting healthcare privacy and security assurance, and communicates throughout the organization to increase awareness and ensure that compliance is achieved where required.

- Monitor the external threat environment for emerging threats, and advise relevant stakeholders on the appropriate courses of action.
- Responsible for conducting training and communications plans and programs which includes security awareness, security training, security training compliance, security reminders, and new hire security orientation.

Qualifications

- Bachelor of Science in related field such as Computer Science, Information Science and Security.
- Compliance and/or IT Certifications (2 or more)
- Minimum of 10+ years of progressively responsible and directly related work experience with at least 6-8 years of leadership experience in an information security management role with increasing levels of responsibility.
- Experience with advising and effectively guiding senior management as to information security matters and demonstrated skill successfully working in a matrixed organization.
- In-depth knowledge of HIPAA Privacy and Security regulations.
- Substantial experience in data auditing processes and methods, cyber-security principles such as CIA (confidentiality, integrity & availability), encryption (including symmetric and asymmetric keys), digital signatures, ports, protocols & services, policies, procedures, physical security, risk management, configuration management, ethics, access control, security architecture, continuity of operations, contingency planning, disaster recovery, application security, and cyber-security rules, laws, and regulations.
- Ability to define and implement a multi-year strategic program and a corresponding set of strategic goals.
- Proven skills and experience with general management, strategic planning, program development and negotiations; skills in analysis, organization, and presentation.
- Knowledge and ability to direct a team in integrating informational technology services with the work requirements and deliverables of units and departments.
- Ability to carry out position with a high degree of discretion, customer service, communication, teamwork, and timeliness.

For more Information / To Apply:

https://careers-ucm.icims.com/jobs/28568/exec-director%2c-chief-information-security-officer/job