Job Code: 101364
Position #: (NUNC) (E)
Developed by: …..… KK
Reviewed by:… LK, DLJ
Approved by: …..…. LK
Date: ……......... 05/19

University of Rhode Island
Position Description

TITLE:	Chief Information Security Officer
DIVISION:	Academic Affairs / Administration and Finance
REPORTS TO:	Chief Information Officer
GRADE:	16
SUPERVISES:	Professional and Technical staff

BASIC FUNCTION:

Establish and maintain the information security program to ensure that information assets and associated technology, applications, systems, infrastructure and processes are adequately protected in the digital ecosystem in which we operate. Identify, evaluate and report on legal and regulatory, IT, and cybersecurity risk to information assets, while supporting and advancing business objectives. Lead the information security program, while coordinating disparate drivers, constraints and personalities, while maintaining objectivity and a strong understanding that cybersecurity is foundational for the university to deliver on its strategic goals and objectives.

As part of the IT leadership team, collaboratively work with ITS partners to secure information assets and associated technology, applications, systems and processes in the wider ecosystem in which the university operates. Actively collaborate with university leadership to determine acceptable levels of risk for the university. Lead, inspire, motivate and evaluate the work of the unit while striving for continuous process improvement and staff professional development.

ESSENTIAL DUTIES AND RESPONSIBILITIES:

In support of Core Responsibilities, facilitate an information security governance structure through the implementation of a hierarchical governance program, including the formation of an information security steering committee or advisory board.

Provide regular reporting on the current status of the information security program to enterprise risk teams, the President’s leadership team as part of a strategic enterprise risk management program, thus supporting business outcomes.

Manage Information Security products, contracts and vendors to ensure timely budgeting, purchasing and renewal processes with a three-year financial projection. Develop and establish total cost of ownership metrics for all services.

Work with the procurement office to ensure that information security requirements are included in contracts by liaising with vendor management and procurement organizations.

Create and manage a targeted information security awareness training program for all employees, contractors and approved system users, and establish metrics to measure the effectiveness of this security training program for the different audiences.

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 privacy, risk management, compliance and business continuity management.

Provide clear risk mitigating directives for projects with components in IT, including the mandatory application of controls.

In the areas of Management and Leadership, provide leadership, vision and direction, in concert with the Strategic Academic Plan, to the Information Security organization to ensure it will contribute to the University achieving its goals.

Work with CIO and other IT leaders to develop overall IT strategy in the context of the Strategic Academic Plan and President's goals.

Lead the information security function across the University to ensure consistent and high-quality information security management in support of the University's goals.

Provide support and facilitate innovative and experimental technology uses to test new ideas with bounded cost and time frames.

Determine the information security approach and operating model in consultation with stakeholders and aligned with the risk management approach and compliance monitoring of nondigital risk areas.

Manage the cost-efficient information security organization, consisting of direct reports and dotted line reports (such as individuals in business continuity and IT operations), including hiring (and conducting background checks), training, staff development, performance management and annual performance reviews.

Manage group personnel, developing their skills and capabilities to meet the needs of the organization, as well as building on existing recruiting capabilities to address new needs and skills gaps. Lead group through change as IT approaches and tools evolve.

Work to develop a group culture of respect, responsiveness, and mutual support of other team members, other ITS departments, distributed IT and the faculty and staff of other divisions.

In support of Service Governance, Strategy and Delivery, work with stakeholders and governance groups to define a prioritized set of functional outcomes and service work to accomplish those outcomes within the limitations of the budget. Work with stakeholders to accomplish this service work in a way that improves service delivery and minimizes its ongoing support costs.

Oversee the unit's successful delivery of these outcomes in partnership with colleagues.

Develop an information security vision and strategy that is aligned to organizational priorities and enables and facilitates the organization's business objectives, and ensure senior stakeholder buy-in and mandate.

Develop, implement and monitor a strategic, comprehensive information security program to ensure appropriate levels of confidentiality, integrity, availability, safety, privacy and recovery of information assets owned, controlled or/and processed by the University.

Assist with the identification of non-IT managed IT services in use ("citizen IT") and facilitate a university IT onboarding program to bring these services into the scope of the IT function, and apply standard controls and rigor to these services; where this is not possible, ensure that risk is reduced to the appropriate levels and ownership of this information security risk is clear.

Work effectively with business units to facilitate information security risk assessment and risk management processes, and empower them to own and accept the level of risk they deem appropriate for their specific risk appetite.

OTHER DUTIES AND RESPONSIBILITIES:

Create the necessary internal networks among the information security team and line-of-business executives, university compliance, audit, physical security, legal and HR management teams to ensure alignment as required.

Build and nurture external networks consisting of industry peers, ecosystem partners, vendors and other relevant parties to address common trends, findings, incidents and cybersecurity risks.

Liaise with external agencies, such as law enforcement and other advisory bodies, as necessary, to ensure that the organization maintains a strong security posture and is kept well-abreast of the relevant threats identified by these agencies.

Liaise with the university infrastructure services team to build alignment between the security and enterprise (reference) architectures, thus ensuring that information security requirements are implicit in these architectures and security is built in by design.

Conduct the majority of work at the Kingston campus of the University of Rhode Island.

Be an active presence in meetings. Be available for staff and collaborators for in-person consultation. Build essential relationships.

Attend national and international conferences, seminars and similar events. Stay up to date on important and constantly evolving aspect of IT operations at a major research University. Travel as necessary.

LICENSES, TOOLS AND EQUIPMENT:

Desktop software and work management tools, computer workstation uses, Information Technology terminology and service delivery practices.

ENVIRONMENTAL CONDITIONS:

This position is not substantially exposed to adverse environmental conditions.

QUALIFICATIONS:

REQUIRED: Bachelor's degree in computer science, engineering, finance, business management or a related field; Minimum of five years group management experience in higher education; Demonstrated ability to manage a high-performing, cohesive team; Demonstrated knowledge and understanding of relevant legal and regulatory requirements, such as: Rhode Island Identity Theft Protection Act of 2015, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLBA) and Payment Card Industry/Data Security Standard; Demonstrated analytical and problem-solving skills; Demonstrated knowledge of business management, information security risk management and cybersecurity technologies; Demonstrated strong interpersonal and verbal communication skills; Demonstrated proficiency in written communication skills; and, Demonstrated ability to work with diverse groups/populations.

PREFERRED: Graduate degree in computer science, engineering, finance, business management or a related field; Demonstrated high degree of initiative, dependability and ability to work with little supervision while being resilient to change; Demonstrated experience leading teams through change as technology and organizational needs evolve through the application of guidance, advice and nonjudgmental leadership techniques; Demonstrated ability to collaborate, build relationships and influence individuals at all levels in a distributed responsibility environment to ensure effective service delivery; Demonstrated understanding of strategic university objectives and a track record of aligning services to support those objectives; Demonstrated ability to deal with rapid change in University needs, processes and technologies; Demonstrated ability to manage multiple competing priorities with limited resources; Demonstrated ability to understand key concepts and communicate effectively with technical staff, application stakeholders and senior leadership, many of whom are in non-technical roles; Demonstrated experience managing external IT service providers, including the risk and cost implications of contracts and contract negotiations; Demonstrated evidence of membership in professional organizations, trade or user groups; and, A pattern of regular attendance at industry conferences to enhance knowledge of current technology.

ALL REQUIREMENTS ARE SUBJECT TO POSSIBLE MODIFICATION TO REASONABLY ACCOMMODATE INDIVIDUALS WITH DISABILITIES.