RHODE ISLAND COLLEGE
JOB DESCRIPTION

Position classification: NUNC
Date created or revised: 9/14/2022
Exempt/Non-Exempt Status: Exempt
Responsible individual: Yes
Campus Security Authority: No

Title:	Director, Information Security
Status:	Full time, 35 hours per week.
Grade:	17
Union Affiliation:	NUNC (Non-Union/Non-Classified)
Reports To:	Assistant Vice President, Information Services

PRIMARY PURPOSE:

The Director of Information Security is responsible for providing leadership for data and information security.   Areas of responsibility include: information security policy, controls, practices, and standards; information security awareness and training; information security incident response and management; risk assessment and management; information security-related IT architecture; and coordination of information security programs to address state and federal statutory and regulatory compliance. Participate actively in Information Security Officer (ISO) groups in higher education and the State of RI.

DESCRIPTION OF DUTIES AND RESPONSIBILITIES:

Essential Job Functions:

- Work closely with all members of the Rhode Island College community. Serve to protect College operations from any data security breaches, unauthorized access and leads the College forward in identity management programs. Key partnerships include Safety and Security, the CIO, the PEC, Capital Planning and Facilities, and Human Resources.
- Develop, implement, monitor and report on a comprehensive “information security blanket” program. Key functional responsibilities are highly integrated.

Operations:

- Develop, implement, and administer technical security standards, as well as a suite of information security services and tools to address and mitigate security risk.
- Ensure disaster recovery and business continuity planning processes are in place and receive regular review for currency and adequacy.
- Lead efforts to internally assess, evaluate, and make recommendations to management regarding the adequacy of the security controls for the University's information and technology systems.

Projects:

- Assure an organizational structure and working environment to support a service orientation and coordination of campus resources, planned change, and continuous improvement.
- Provide leadership, direction, and guidance in assessing and evaluating information security risks and monitor compliance with security standards and appropriate policies.
- Examine impacts of new technologies on the College’s overall information security. Establish processes to review implementation of new technologies to ensure security compliance.

Architecture:

- Define, implement, and upgrade a Unified Threat Management system for the College. Services therein include firewalls, access control, intrusion protection, identity management, encryption and more.
- Oversee processes for configuration management, change management and vulnerability management.
- Lead the development and implementation of effective and reasonable policies and practices to secure protected and sensitive data.

Planning:

- Lead information security planning processes to establish an inclusive and comprehensive information security program for the entire institution in support of academic, research, and administrative information systems and technology.
- Establish annual and long-range security and compliance goals, define security strategies, metrics, reporting mechanisms and program services; and create maturity models and a roadmap for continual program improvements.
- Serve on College committees, councils, and boards as requested by the Vice President of Administration and Finance.
- Participate in institutional security collaborations and higher education security groups.
- Maintain an expert working knowledge and technical understanding of the College networks, applications, data, services, and products.

Compliance:

- Lead the development and implementation of effective and reasonable policies and practices to secure protected and sensitive data and ensure information security and compliance with relevant legislation and legal interpretation.
- Maintain a comprehensive working knowledge of federal, state, and local laws and regulations, and industry standards where compliance requires specific data and information security policies, practices, reporting or audits. These include, but are not limited, to HIPAA, FERPA, HEOA, DMCA and PCI DSS.
- Ensure that College policies reflect all matters and responsibilities for information security.
- Conduct periodic security audits of the IT environment; develop reports, document results and recommend changes; supervise implementation plans.
- Lead incident response efforts including forensics and investigations in the event of a data breach or incident. Create a SIRT (Security Incident Response Team) as needed or requested.

Communications:

- Establish and manage an evergreen information security campaign for faculty, staff, and students including training and personal responsibility for all in information security management. Create education and awareness programs and advise operating units at all levels on security issues, best practices, and vulnerabilities.
- Maintain a high level of community empathy and understanding of the College’s mission and the work of faculty, students, and staff sufficient to ensure a secure technology environment that enables learning innovation, student success, inclusive excellence, community partnerships, and institutional effectiveness.
- Pursue student security initiatives to address unique needs in protecting identity theft, mobile social media security, and online reputation program.

REQUIRED QUALIFICATION STANDARDS:

Education:

Advanced degree in Computer Science, MIS, Business, or a closely-related field with minimum of five years of significant administrative experience managing technology initiatives and services.

OR

Bachelor's degree with minimum of eight years of significant administrative experience managing technology initiatives and services.

Experience:

- Experience must include successful administration of technology initiatives in a complex environment
- Successful experience integrating information systems, as well as resources and services in support of academic and/or administrative functions.
- Leadership experience managing information and instructional technologies as well as infrastructure and networking.

Skills, Knowledge, and Abilities:

- Significant information technology leadership and management experience applying computing and information technologies in support of administrative and/or academic objectives.
- Evidence of creativity, flexibility, innovation, and vigorous leadership.
- Workstations and multiple operating systems, network testing, monitoring and sniffing tools; system and network vulnerability (hacking) tools; CISSP, GIAC or comparable certification; intrusion detection system experience, PKI and certificate management experience; Cisco routers and switches.
- Working knowledge of network security technologies such as VPN, firewall, and WLAN as well as computer security technologies for UNIX and PC systems such as antivirus, WLAN security, and middleware
- One or more applicable Information Security certifications such as Certified Information Systems Security Professional (CISSP).
- Change management skills.
- Strong service commitment to clients.
- Demonstrated ability to advance innovative data and information security programs in response to a rapidly changing information technology environment.
- Excellent interpersonal, communication and collaborative skills.
- Demonstrated ability to build team support.
- Understanding of the mission, role, and operations of data management and information technologies.

PREFERRED:

- Experience in a higher education environment, with the technology infrastructure.

- CISSP or other credentials.

- Master’s degree in computer science or related field.
- Direct experience as a manager of information security for an organization.
- Experience in developing information security policies, guidelines, and best practices; CISSP, GIAC or comparable certification.
- Intrusion detection system experience.
- PKI and certificate management experience.
- Experience with Cisco routers and switches.
- Bilingual in English / Spanish (fluent in speaking and writing).

ENVIRONMENTAL CONDITIONS:

The employee is not exposed to known adverse environmental conditions.

The College requires that all applicants and employees be able to perform the essential functions of the job and will explore reasonable accommodations for individuals with disabilities.

As an Affirmative Action/Equal Opportunity institution that values and is committed to inclusion and expanding the diversity of its faculty and staff, the College invites members of protected classes, including minorities and persons with disabilities, to identify themselves as such at the time of application.