COMMUNITY COLLEGE
OF RHODE ISLAND
Division of Institutional Equity and Human Resources

POSITION DESCRIPTION

TITLE	Director of Information Security
POSITION NO.	502362
LOCATION	Warwick
REPORTS TO	Interim CIO & Director of Enterprise Applications
GRADE	BOE 18
WORK SCHEDULE	Non-Standard: 35 hours per week, evening and weekend; additional hours required. May require travel between campuses.
REVISION DATE	November 2016

JOB SUMMARY:
The Director, Information Security will build and lead our security team, evolve our security and compliance programs, and partner across the college in all things related to security. This role will lead a team of specialists responsible for governance, risk, compliance, and cybersecurity aspects of our security program. The ability to influence and partner closely with other groups on multi-functional initiatives is a top requirement, including oversight of security audits and domestic and international compliance/privacy laws and regulations (NIST, GDPR, FERPA, CCPA, etc.). This individual will report directly to the Chief Information Officer and will be a key leader on the Information Technology team.

DUTIES AND RESPONSIBILITIES:

- Influence, guide, and lead compliance programs in accordance with industry standards and requirements such as NIST, GLBA, FERPA, and GDPR among others.
- Develop, implement and maintain college policies, procedures, measures and mechanisms to protect the confidentiality, integrity and availability of all data and to prevent, detect, contain, and correct information security incidents by aligning information security standards and compliance with legal and regulatory requirements.
- Ensure disaster recovery and business continuity plans are in place and tested.
- Develop, maintain, and evolve the college's security policies and testing program, conduct security audits and evaluations of prospective vendors/partners and work with outside consultants, as appropriate, for independent security audits.
- Be responsible for the security incident response program, conducting threat and vulnerability assessments, serving as the chairperson of the team, investigating actual or potential security incidents or breaches and implementing associated disciplinary and legal responses.
- Maintain a current understanding of the IT threat/risk landscape.
- Brief the executive team on status and risks, including taking the role of champion for the overall strategy and required budget. Also prepare update reports and performance metrics for Senior Management.
- Develop information security-related training and education programs, including on the college's policies and procedures, and work with the human resources department to deliver training to staff on a regular basis.
- Evaluate, select, implement and prioritize security products and technologies.
- Monitor security and privacy trends in the SaaS / cloud technology space and provide timely educational resources to the various CCRI teams to stay on top of relevant laws and legislation and to ensure that the security and privacy programs are updated to maintain ongoing compliance.
- Identify potential areas of vulnerability and risk. Facilitate the formulation of corrective action plans for resolution of problematic issues, while maintaining an acceptable level of risk.
- Ensure the security controls for computer equipment (laptops, mobile devices, BYOD).

LICENSES, TOOLS, AND EQUIPMENT:
All modern office equipment and software, including but not limited to Microsoft Office, PowerPoint, Excel and Word.

ENVIRONMENTAL CONDITIONS:

This position is not substantially exposed to adverse environmental conditions.

REQUIRED QUALIFICATIONS:

- Bachelor's Degree in Business, Computer Science or Information Systems preferred
- Experience in a SaaS organization highly preferred.
- 5-10 years of demonstrated ability in the Information Security field.
- 5+ years' experience with leading information security teams.
- 5+ years of experience working in Cloud solutions and architectures.
- 3+ years of experience working across Senior Management and presenting to C-Suite and Board Level Executives.
- Deep understanding of: SecOps (Security Operations), Security architecture, SaaS/Cloud infrastructure security, and Secure SDLC.
- Experience implementing information security industry and frameworks, specifically NIST.
- Experience with RFP/InfoSec assessments for SaaS solutions.
- Experience with Program/Project Management methodologies.

PREFERRED QUALIFICATIONS:

- Professional certifications such as CISSP, CISM, and/or CISA preferred.
- Familiarity with SIG tools and practices.
- Knowledge and/or experience with Privacy requirements including GLBA, FERPA, GDPR, and CCPA**.**

All requirements are subject to possible modification to reasonably accommodate individuals withdisabilities.