COMMUNITY COLLEGE
OF RHODE ISLAND

Division of Institutional Equity and Human Resources

POSITION DESCRIPTION

TITLE	Engineer Cyber Security
POSITION NO.	501389
LOCATION	Warwick
REPORTS TO	Director Information Security
GRADE	PSA 14
WORK SCHEDULE	Non-Standard: 35 hours per week
SUPERVISION	
LIMITATION (if applicable)	N/A
REVISION DATE	August 2023

JOB SUMMARY:

The Cyber Security Engineer, reporting to the Director of Information Security, will lead the implementation of a robust cyber security program in collaboration with internal and external teams. They will focus on creating comprehensive documentation, assessing processes, resolving security issues, and refining security standards to meet CCRI & regulatory requirements. By working closely with IT service delivery teams, they will ensure the confidentiality, integrity, and availability of information assets. The engineer will actively detect, assess, and respond to cybersecurity events within the college's data processing environments, while also managing audit support tasks and proactively identifying indicators of compromise. In partnership with application owners, IT staff, and CCRI partners, they will mitigate security threats. Effective interaction with product vendors, service providers, and personnel from various college departments and business units is essential for success in this role.

DUTIES AND RESPONSIBILITIES:

- Manage the lifecycle of vulnerabilities, from discovery and triage to remediation and validation.
- Continuously review and update security systems documentation to ensure accuracy and relevance.
- Stay abreast of industry standards, regulations, and emerging threats, incorporating them into security practices and strategies.
- Foster effective relationships with key stakeholders to facilitate collaboration and support for IT security initiatives.
- Design, improve, and manage testing scripts, tools, and processes for data processing environment security assessments.
- Coordinate scoping, scheduling, and logistics for penetration tests and security assessments, coordinating with product owners.
- Conduct penetration tests and vulnerability assessments to evaluate the effectiveness and resilience of the college's information systems and infrastructure, while identifying and exposing weaknesses.
- Collect and analyze security incident and event data to generate exception and incident reports.
- Work with data to collect, summarize, and visualize compliance evidence reporting.

LICENSES, TOOLS, AND EQUIPMENT:

ENVIRONMENTAL CONDITIONS:

This position is not substantially exposed to adverse environmental conditions.

REQUIRED QUALIFICATIONS:

- Bachelor's degree.
- Minimum two years of experience in an Information Security role.
- Minimum two years of experience working on corporate technologies (including but not limited to endpoints, servers, and network technologies).
- Demonstrated experience with vulnerability management solutions, MDM technologies and endpoint security solutions.
- Demonstrated experience securing multiple operating systems.

- Demonstrated knowledge of networking and application protocols.
- Demonstrated customer service skills and technical problem-solving skills.
- Demonstrated strong interpersonal and verbal communication skills.
- Demonstrated proficiency in written communication skills.
- Demonstrated ability to work with diverse groups/populations.

PREFERRED QUALIFICATIONS:

- Master's degree.
- Demonstrated higher education experience in a security administrator position.
- Demonstrated knowledge of cloud platforms and cloud security.
- Demonstrated experience in regulated environments (HIPAA, PCI, GLBA, etc.).
- Demonstrated experience with data loss prevention technologies.
- Demonstrated experience with web application security scanners.

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