Job Code: 101603
Position #: (PSA).....(E)
Developed by:..... MK
Reviewed by:..... DLJ
Approved by:.....LK
Date: 10/13/22

University of Rhode Island
Position Description

Title:	Cyber Security Engineer
Division:	Academic Affairs / Administration and Finance (ITS)
Reports To:	Chief Information Security Officer
Grade:	14
Supervises:	Technical staff

BASIC FUNCTION:

Partner with internal and external teams to manage cyber security tools including but not limited to allow list technologies, data loss prevention, malware prevention and real time metrics reporting. Establish and maintain the secure configuration of endpoint devices, ensuring compliance with the secure configuration of university endpoints. Assist with project teams to implement and tune new patch management processes / technologies into the URI working environment. Work with URI constituents on providing product updates, bug fixes and managing relations. Create clear and concise documentation to formalize new processes. Process requests to resolve endpoint security issues with endpoint support and end users which also includes exception / exclusion handling. Administrate and implement policies / rules on endpoint devices as well as refine security standards. Implement and maintain cyber security management tools for endpoint protection. Interact closely with product vendors and service providers, with personnel from various IT departments (including the application development, infrastructure, network, and with business units and colleges).

ESSENTIAL DUTIES AND RESPONSIBILITIES:

Provide technical support, including monitoring, reporting, and tool administration.

Design and integrate endpoint protection solutions in the university's infrastructure based on the ongoing business requirements and those of URI's security policy.

Keep security systems documentation up to date.

Maintain awareness of latest security risks, exploits, and vulnerabilities and apply them to the URI environment as required.

Ensure the automation of both operating system and application patch management on a monthly or more frequent basis.

Build effective relationships with key stakeholders who own and support IT infrastructure, applications, processes, and operations.

Examine systems and applications to assess the current security posture.

Perform comprehensive vulnerability assessments and continuous monitoring across the university.

Manage the entire lifecycle of vulnerabilities from discovery, triage, advising, remediation, and validation.

Raise concerns to management regarding endpoint security deficiencies or enhancements that need to be addressed.

Develop, maintain, and monitor endpoint security technology and best practices and provide ongoing monitoring of new technology and capabilities.

Possess and maintain broad technical and business knowledge of all aspects of endpoint technologies including mobility, client operating systems, VDI, and IOT.

Possess broad expertise with client and endpoint authentication (SSO), data protection, VPN, antivirus, and anti-malware technologies and controls.

Oversee the implementation, administration, and operation of multiple endpoint security technologies such as but not limited to Absolute, Cylance, Patch Management, Bitlocker and Filevault.

Work with the Manager of Endpoint Support to design and implement a stable, secure, and optimized endpoint environment for university constituencies.

OTHER DUTIES AND RESPONSIBILITIES:

Perform other duties as assigned.

LICENSES, TOOLS, AND EQUIPMENT:

Desktop software and work management tools, computer workstation, Information Technology terminology and service delivery practices. Project management and general IT Service Management tools.

ENVIRONMENTAL CONDITIONS:

This position is not substantially exposed to adverse environmental conditions.

QUALIFICATIONS:

REQUIRED: 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 (e.g., Qualys, Tenable, Rapid7, etc.) and with MDM technologies (e.g., Microsoft Intune); Demonstrated experience with endpoint security solutions (e.g., Absolute, Cylance, Cisco Umbrella, etc.), best practices and procedures; Demonstrated deployment and maintenance experience with endpoint security solutions (including anti-virus, anti-malware, disk encryption, EDR, DNS security, patch management); Demonstrated experience securing multiple operating systems (e.g., Mac, Windows, Linux and/or other Unix-like variants): Demonstrated knowledge of networking and application protocols (e.g., TCP/IP, UDP, HTTPS); Demonstrated customer service skills and technical problem-solving skills; Demonstrated strong interpersonal and verbal communication skills; Demonstrated proficiency in written communication skills; and, Demonstrated ability to work with diverse groups/populations.

PREFERRED: Master's degree; Demonstrated higher education experience in a security administrator position; Demonstrated ability to automate and script tasks using preferred language; Demonstrated ability to work with remote data and write scripts against common web APIs (REST, SOAP); Demonstrated knowledge of cloud platforms and cloud security; Demonstrated experience in regulated environments (HIPAA, PCI, GLBA, etc.); Demonstrated understanding of endpoint security, operating systems, networks, and application layer technologies; Demonstrated experience with data loss prevention technologies; Demonstrated experience with desktop administration and troubleshooting; and, Demonstrated experience with web application security scanners (e.g., Qualys, Tenable, Rapid7, etc.)

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