Classification Level:	Administrator
Original Date:	January 21, 2020
Revision Date:	April 1, 2024 October 27, 2025 May 12, 2026
Pay Group:	11

JOB DESCRIPTION

MANAGER, CYBERSECURITY OPERATIONS

JOB RESPONSIBILITIES

Reporting to the Director of DTO and Cybersecurity, Digital Technology Services, (DTS) and a part of the Associate Vice President (AVP) DTS leadership team, the Manager, Cybersecurity Operations leads the cybersecurity team that provides security operations, incident response, and security controls to digital solutions across the university.

This role will have the opportunity to influence and drive lasting efforts in the University's digital transformation, with significant student and employee impact through the management and monitoring of a robust cybersecurity program and development of policies relating to digital solutions. In close alignment with university wide strategy, critical components of this position include updates to the Cybersecurity strategy, risk management framework, vulnerability management program, Cybersecurity protection, Cybersecurity access controls, Cybersecurity detection and incident response plan. The role requires a strong focus on building and maintaining relationships both across the CapU community and externally with sector colleagues and vendors.

KEY RESPONSIBILITIES:

- In consultation with the Director, DTO and Cybersecurity, plans implements, and manages security controls, operations and response that is guided by cybersecurity frameworks, critical security controls and the National Cybersecurity Assessment (NCA) framework.
- Develops and maintains cybersecurity training material and manages role-based specific cybersecurity training, monitors, and reports compliance to cybersecurity training across the university community
- Performs follow up with university community members who are not compliant, including managing the refresher program.
- Proactively contributes to technical assessments from a cybersecurity perspective of all digital solutions that are being selected for the digital ecosystem. This includes providing security requirements and performing evaluations from a cybersecurity perspective for RFPs.
- Develops and manages the cybersecurity sections of technical assessments.

- Leads and coordinates an appropriate level of response to cybersecurity alerts and incidents, including the implementation and review of a cybersecurity incident response plan.
- Identifies and selects appropriate cybersecurity monitoring tools to ensure no gaps exist in security management across the digital ecosystem.
- Proactively monitors the digital ecosystem using industry standard tools to detect malware, suspicious activity, and breaches across all levels of the digital ecosystem, including network, services and applications.
- Updates processes and tools, seeking to consistently improve the program. Works closely with the Manager(s) of cybersecurity programs to ensure that all policies, guidelines, controls relating to cybersecurity and DTS are maintained annually.
- Identifies, manages, and responds to security breaches, coordinating with DTS leadership team to ensure there are appropriate resources allocated and communications prepared.
- Manages and continuously follows up on any risks identified with security operations, training, and technical assessments to ensure they are mitigated and resolved.
- Analyzes, investigates, and evaluates emerging cybersecurity technology and software trends, including product road maps, to determine impact on DTS roadmap.
- Builds working relationships and partnerships across the university community and sector, providing expert advice on committees, initiatives and engaging with external communities of practice.
- Manages vendor relationships, including development of RFPs, evaluation of proposals, and management of vendor performance, support agreements and licensing.
- Contributes to team development through engaged mentorship and knowledge sharing to help team members grow their cybersecurity experience and skills.

KEY COMPETENCIES:

- Job knowledge: knowledge and experience with cybersecurity best practices; demonstrates proven leadership experience in developing strategies, plans, programs and policies related to the delivery of cybersecurity strategy and operations.
- Service focus: understands the role of cybersecurity and digital solutions, and how change affects teams and processes; delivers services that align with the DTS roadmap that support the university's key priorities of exceptional student and employee experience.
- Result oriented: feels personally committed and accountable to deliver results quickly, accurately, and effectively; uses thoughtful judgement when responding to situations that are not going well and uses foresight to overcome obstacles.
- Initiating action / taking initiative: embraces a continuous improvement mindset in an

ongoing effort to improve services and processes; readily acts consistent within departmental or university objectives; volunteers readily and takes independent actions when appropriate.

- Leadership and supervisory abilities: encourage and supports cross-functional, high-performing teams; attracts and selects the best talent; coaches and inspires people; sets expectations, recognizes achievement, and proactively manages conflict.
- Problem solving and decision-making: ability to understand complex systems and processes and find diverse solutions to stubborn problems; makes clear, consistent, and transparent decisions; acts with integrity in all decision making.
- Strategic planning and organizing: Demonstrated capacity to develop and implement strategies, tactical plans, policies, and procedures. Experience managing a cybersecurity program.
- Employee development: achieve desired organizational results by encouraging and supporting the contribution of others; modeling positive leadership behaviours, including integrity, honesty, a sense of urgency and leading by example.

REQUIRED EDUCATION/TRAINING AND EXPERIENCE

- 5+ years of relevant professional experience, with 1 years in a recent leadership role with direct responsibility for a cybersecurity program, preferably in a public sector environment.
- Demonstrated experience in leading a cybersecurity program.
- Demonstrated experience and knowledge of cybersecurity processes, tools, and procedures, including policies and establishing governance structures.
- A bachelor's degree
- Industry relevant designations such as CISSP, CISA, CRISC, ITIL, TOGAF.
- Experience with the ITIL framework and ITSM best practices, tools, and techniques; ITIL certification is an asset.
- Broad technical knowledge relating to cybersecurity practices, including patching, firewalls, network configurations, phishing, and software deployment.
- Demonstrated experience in effectively communicating and presenting cybersecurity risks to varies levels within an organization.
- Demonstrated experience in developing policies relating to a digital technology department, including cloud based.
- Completion of a criminal record check.