Classification	Administrator
Original Date:	
Revision Date:	April, 2024
Pay Group:	11

MANAGER, IDENTITY AND ACCESS SERVICES

JOB RESPONSIBILITIES

Reporting to the Senior Manager, Central Cybersecurity Services,and a part of the Associate Vice President (AVP) DTS leadership team, the Manager, Identity and Access Services leads the cybersecurity team that provides identity management and access 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 identity and access management program across digital solutions. In close alignment with university wide strategy, critical components of this position includes: alignment of the identity and access management program with 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 and the Senior Manager Central Cybersecurity Services plans, implements, and manages the identity and access management program that is guided by developed cybersecurity frameworks, critical security controls and the National Cybersecurity Assessment (NCA) framework.
- Develops and manages identity and access management processes to ensure appropriate access to all digital solutions. This includes but is not limited to access to data backups, restores, and data archives.
- Proactively manages and maintains the Microsoft Identity Management (MIM) and Active Directory FS (ADFS).
- Develops and manages the onboarding/offboarding process to the network and DTS services ensuring access is prohibited for unauthorized use and cybersecurity policies are enforced.
- Develops and manages the single sign on and authentication process for systems.
- Develops and maintains role-based security matrix for access to digital solutions across the university community.
- Participates and provides the appropriate level of response to security breaches including incident response.

- Updates identity management and access processes and tools, seeking to consistently improve the program. Works closely with the Manager, Cybersecurity and Policy Advisor to ensure that all policies relating to identity and access of digital solutions are maintained annually.
- Working with the centralized security services team, Identifies and selects appropriate cybersecurity monitoring tools relating to auditing and assessments to ensure no gaps exist in security management across the digital ecosystem.
- Working with the Manager, Digital Services, develops auditing protocols to periodically audit identity and access across the digital ecosystem.
- Identifies and reports cybersecurity risks through the identity management and access program to the Director, DTO and Cybersecurity and Manager Centralized Security Services for appropriate risk management.
- Develops and guides standards relating to identity and access controls.
- Manages and continuously follows up on any risks identified with identity and access to ensure they are mitigated and resolved.
- Manages the administration and configuration of identity management and access control systems. Coordinates platform updates and upgrades.
- Manages and oversees the technical identity and access management architecture, including authorization and authentication methods.
- Analyzes, investigates, and evaluates emerging cybersecurity technology and software trends, including product road maps, to determine impact on DTS road map.
- 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.
- Other duties and responsibilities as assigned.

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.

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 identity and access management processes, tools, and procedures.
- A Bachelor's degree
- Industry relevant designations such as CISSP, CISA, CRISC, ITIL, TOGAF.
- Experience in Microsoft Identity Management (MIM) and Active Directory FS (ADFS). Azure security architecture knowledge.
- 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 identity and access management information to varies levels within an organization.
- Demonstrated experience in developing role-based matrix for a mid-large size organization.
- Completion of a criminal record check.