Job Description

Position Title: Assistant Director, Cybersecurity

Job Family: Information Technology

Job Level: Manager

FLSA Status: Exempt

Salay Grade: 10

Position Summary:

The Cybersecurity Assistant Director is responsible for providing high-level technical leadership, operational direction, and project management for the college's enterprise-wide security program. This position is accountable for the protection of institutional data, systems, and digital assets. The Assistant Director coordinates major security initiatives, manages risk, and ensures compliance with institutional policies and industry standards and frameworks. This role requires the ability to work with minimal supervision, lead incident response efforts, and provide technical guidance to the IT leadership team.

The Cybersecurity Assistant Director may be assigned to the following areas:

Security Operations: This position oversees the college's active threat defense and the security of its technical infrastructure. The primary area of expertise centers on high-tempo tactical execution, continuous threat monitoring, incident response, and infrastructure hardening. Responsibilities include overseeing network and endpoint defense, firewall administration, SIEM management, automation engineering, and acting as the tactical leader during cyber crises to ensure rapid incident triage, containment, and system recovery.

Identity, Access Management (IAM), and Digital Investigations: This position oversees the college's digital identity lifecycle (including non-human identities), access controls, system access, security training, and confidential forensic investigations. The primary area of expertise focuses on compliance, identity governance, and methodical investigative processes. Responsibilities include managing multi-factor authentication (MFA), federated access environments, single sign-on to all the college's applications, and enterprise-wide identity protocols, while also directing meticulous digital investigations and eDiscovery efforts that require close coordination with human resources and legal stakeholders. Special consideration is given to agentic AI, where a single individual identity (a single employee) can now spawn into the 10s and 100s of agent identities throughout the environment.

Essential Duties and Responsibilities:

Examples of key duties are interpreted as being descriptive and not restrictive in nature. Incumbents routinely perform approximately 80% of the duties below.

1. Manages assigned cybersecurity personnel and security operations, including incident response and proactive threat hunting. Provides work direction, technical guidance, mentorship, performance management, and professional development to build advanced technical capabilities within the team.
2. Oversees and performs advanced cybersecurity administration across network, endpoint, server, and cloud environments. Designs, implements, and maintains security controls and defense-in-depth strategies to protect the confidentiality, integrity, and availability of institutional systems, data, and digital assets.

3. Leads and performs complex cybersecurity incident response activities, including investigation, containment, isolation, forensic analysis, root cause analysis, recovery, and post-incident review. Coordinates backup and recovery activities associated with cybersecurity incidents.
4. Manages and administers identity and access management and data protection controls, including multi-factor authentication, single sign-on, identity governance, access control frameworks, Data Loss Prevention (DLP), and enterprise email security. Develops and enforces related cybersecurity policies, standards, and procedures.
5. Configures, administers, tunes, and provides technical oversight of enterprise cybersecurity infrastructure, including firewalls, Security Information and Event Management (SIEM) systems, security automation and orchestration platforms, and related security technologies. Evaluates and advises on the security posture of the College's technology environment.
6. Leads vulnerability management, attack surface management, and continuous security monitoring activities. Identifies, assesses, prioritizes, and mitigates vulnerabilities and cybersecurity risks across institutional technology environments, including operating systems and externally accessible assets.
7. Develops, implements, and maintains cybersecurity procedures and technical controls related to system hardening, incident response, disaster recovery, security contingency planning, and the cybersecurity components of business continuity.
8. Serves as a senior technical resource to the CISO and collaborates with IT leadership to align cybersecurity operations and initiatives with institutional goals. Evaluates complex cybersecurity risks and technical issues, develops recommendations, and prepares reports and other information to support leadership decision-making.
9. Develops and administers enterprise-wide cybersecurity training and awareness initiatives designed to reduce human-centered cybersecurity risks and promote secure practices throughout the College.
10. Leads complex cybersecurity projects from requirements definition and design through testing, implementation, documentation, and operational transition. Coordinates project activities and resources and communicates project status, risks, issues, and outcomes to appropriate stakeholders.
11. Participates in the development and administration of cybersecurity budgets and resource planning; evaluates security technology and resource needs, supports procurement and vendor management activities, and monitors the effective use of cybersecurity resources.
12. Performs all other duties and responsibilities as assigned or directed by the supervisor.

Knowledge, Skills, and Abilities:

1. Knowledge of business management and fiscal practices
2. Knowledge of computer and network operating systems
3. Knowledge of project management principles, processes, and techniques
4. Knowledge of regulatory compliance principles and practices
5. Knowledge of server administration, system security, and network design
6. Skill in budget/resource management
7. Skill in coordinating and monitoring the work of others
8. Skill in independent decision making
9. Skill in people leadership and supervision

10. Skill in organization, coordination, and management
11. Skill in problem solving
12. Skill in program development and process improvement
13. Skill in project management principles, processes, and techniques
14. Skill in team building
15. Skill in verbal and written communication with the ability to explain technical concepts to audiences with a wide range of technical skills
16. Skill in current and applicable hardware, software, and peripheral equipment
17. Skill in current and applicable server administration, system security and network design
18. Ability to adapt and maintain professional composure in emergent and crisis situations
19. Ability to develop and maintain effective and positive working relationships
20. Ability to adapt to a rapidly changing technical environment
21. Ability to apply analytical and critical thinking skills with the ability to draw conclusions and prepare accurate reports of results
22. Ability to work independently as well as in a team environment

Supervision:

- Supervises work of others, including planning, assigning, scheduling, and reviewing work, ensuring quality standards. Is responsible for hiring, terminating, training, and developing, reviewing performance, and administering corrective action for staff.

Independence of Action:

- Results are defined; employee sets own goals and determines how to accomplish results with few or no guidelines to follow, although precedents may exist; supervisor/manager provides broad guidance and overall direction.

Competencies:

Competencies are the actions and behaviors that can be observed as to how work gets done that supports the College's values and strategic objectives.

- Information and Analytics: Allows ability to be a data leader. Provides a holistic representation of College's performance as well as data trends or issues.
- Institutional Infrastructure: Allows participation in the development of foundational aspects of the College, including the establishment of a strategic plan, financial and facilities management, accreditation, and technology planning.

Minimum Qualifications:

Candidates/incumbents must meet the minimum qualifications as detailed below.

- Bachelor's degree in Information Technology or a closely related field of study required.
- Master's degree in Computer Science or a closely related field of study preferred.
- Three (3) to Five (5) years of related experience required.
- Five plus (5+) years of related experience preferred.
- One (1) to Three (3) years of supervisory experience required.
- OR An equivalent combination of certification, education and experience sufficient to successfully perform the essential duties of the job such as those listed above.

Physical Demands:

The physical demands described here are representative of those that must be met by an employee to successfully perform the key duties and responsibilities of this job. **Reasonable accommodations may be made to enable individuals with disabilities to perform critical tasks.**

- **Environment:** Work is performed primarily in a standard office environment with staff contact and frequent interruptions.
- **Physical:** Primary functions require sufficient physical ability and mobility to work in an standard office setting; to remain in a stationary position for prolonged periods of time; to occasionally position self to perform duties; to move, transport, and/or position objects of light to moderate (up to 20 pounds) amounts of weight; to operate office equipment including use of a computer keyboard; to travel to other locations using various modes of private and commercial transportation; and to effectively communicate to exchange information.
- **Vision:** Ability to see in the normal visual range with or without correction.
- **Hearing:** Ability to hear in the normal audio range with or without correction.

Special Conditions of Employment:

- Pre-employment Background Check Required
- DMV Check/Current and Valid AZ Driver's License
- Some evening or weekend work hours
- On-call rotation duties