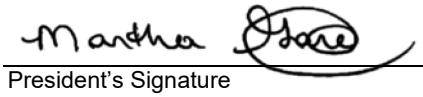
Job Description(s) for President's Cabinet Review

Job Description	
Title:	Information Security Analyst
Unit:	CSEA 262
Range:	A-124
Synopsis:	New
Rationale:	This position is needed to address rising security threats and operational demands. Over the past three months, the organization handled 4,263 security cases, including 33 escalations requiring coordination with the CDT Security Operations Center, highlighting the need for a dedicated point of contact. Phishing attacks are increasing and frequently lead to account compromise and service disruptions, requiring faster and more effective responses.
Incumbent:	To be recruited
Approved?	



May 5, 2026

President's Signature | Date

Comments:

INFORMATION SECURITY ANALYST
FLSA: NON-EXEMPT – A-124
$8,813.73 - $11, 248.82/month

DEFINITION

Under direction and oversight, incumbents assigned to this classification perform complex work related to the College's information security program, including testing, analysis, and evaluation of the integrity and confidentiality of enterprise systems, network, assets, and communication technology within the College. Incumbents will assist in identifying, investigating, and defending against information security incidents targeting the College-wide systems and data. This includes reviewing system logs, analyzing network traffic, configuring and updating system and security tools, and troubleshooting information technology systems. Incumbents will also keep apprised of existing and emerging regulations applicable to the College and will ensure board policies, administrative regulations, and departmental procedures are appropriate for continual compliance. **Serves as a technical subject-matter expert in information security, providing risk-based findings and recommendations related to security controls, vulnerabilities, and incident response activities.**

SUPERVISION RECEIVED AND EXERCISED

Receives ~~administrative~~ **general** direction from the assigned managerial personnel. Exercises no direct supervision of staff. May exercise technical and functional direction and training to staff.

CLASS CHARACTERISTICS

Incumbents assigned to this class serve as a primary technical resource for the College-wide information security program. This position focuses on threat mitigation and vulnerability management with exposure and support to all aspects of information security practice. Incumbents in this position should have advanced knowledge of risk identification, protection, and compliance, threat detection, incident response plan development and review, and recovery services to achieve business continuity and resilience. **Applies working technical knowledge of infrastructure components, including servers, networks, cloud services, and identity systems, to assess risk, validate secure configurations, and communicate findings. Emphasizes security analysis, coordination, and execution within established procedures; does not exercise administrative or infrastructure authority; implementation of changes remains the responsibility of appropriate technical owners. Influence is exercised through technical analysis, documentation, and collaboration with Information Technology (IT) teams, system administrators, application owners, and vendors to align security requirements with operational needs and strengthen the College's overall security posture.** This class is distinguished from the Enterprise Network Security Analyst in that the latter is responsible for designing, implementing, and maintaining the College's enterprise network infrastructure, including hardware, operating systems, and desktop/network applications.

EXAMPLES OF ESSENTIAL FUNCTIONS (Illustrative Only)

1. Serves as a core member of the Information Security team, performing assigned information security duties including threat awareness, proactive network traffic analysis, incident response, forensic analysis, and resolution of security incidents.

2. Reviews the disaster recovery and business continuity plans for Information Technology (IT) infrastructure and systems of the College, including hardware and software, networks, processes and procedures, and users.
3. Provides technical direction on information security initiatives and projects.
4. Provides information security-related training and guidance to the college-wide user community; prepares and performs workshops and training on topics of information security.
5. Leads technical efforts in responding to and resolving information security incidents; maintains, refines, and improves the College's data security program.
6. Evaluates existing and emerging best practices, regulations, and laws to ensure continual compliance.
7. ~~Builds~~ **Collaborates on and maintains** a security environment that reduces and mitigates risk utilizing knowledge of network protocols, services, threats, vulnerabilities, mitigation strategies, hardware capabilities, and other information.
8. Evaluates data to detect security incidents; takes timely action as appropriate to mitigate malicious traffic, create alerts, and/or investigate when suspicious activity is detected; maintains confidentiality of sensitive information security matters.
9. Reviews and **recommends** updates **to** procedures, guidelines, and methods to detect and mitigate security attacks.
10. Participates in response and remediation efforts to information security incidents throughout the College, including post-incident recovery assessment and coordination with support providers; **assists in** develop~~s~~**ing** and implement~~s~~**ing** ~~enforcement~~ policies, procedures, and associated plans for secure system administration and development, and user system access based on industry-standard best practices.
11. Collaborates with College technology staff on security issues; promotes a strong information security culture throughout the College.
12. Conducts assessments of information systems security requirements, evaluates current security posture, and recommends solutions and priorities for remediation.
13. Evaluates and collaborates with vendors and contractors on College information security initiatives to ensure compliance with policies, regulatory requirements, and best practices for data protection and system security.
14. Researches and evaluates information security laws and regulations, including but not limited to Gramm-Leach-Bliley Act, Payment Card Industry Data Security Standard, Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, and their impact on the College.
15. Promotes an environment of belonging as it relates to diversity, equity, inclusion, social justice, anti-racism, and accessibility.
16. Provides quality customer service when interacting with the public, vendors, students, and College staff, including individuals from minoritized groups.
17. Supports and abides by federal, state, and local policies and Board Policies and Administrative Procedures.
18. Participates on committees, task forces, and special assignments, including, but not limited to, Screening and Selection Committees and mandated trainings as required.
19. Prepares and delivers oral presentations related to assigned areas as required.
20. Performs other related or preceding classification duties as assigned.

QUALIFICATIONS

Knowledge of:

1. Principles and practices of supporting a diverse, equitable, inclusive, socially just, anti-racist, and accessible academic and work environment.
2. Data encryption techniques, including but not limited to Public Key Infrastructure.
3. Incident response procedures and computer system forensics.
4. Best practices for applying and maintaining role-based access controls to College systems, technologies, identities, and service providers.
5. Security best practices of servers, Local Area Network (LAN) and Wide Area Network (WAN) networks, virtualization, and Cloud.
6. Secure software development best practices.
7. Security assessment, security auditing, and security testing tools.
8. Methods and techniques of technical documentation and record keeping.
9. Applicable federal, state, and local laws, regulatory codes, ordinances, and procedures relevant to assigned area of responsibility.
10. Modern office practices, methods, and computer equipment and applications related to the scope of responsibility.
11. Techniques for effectively representing the College in contacts with governmental agencies, community groups, and various business, professional, educational, regulatory, and legislative organizations.
12. Techniques for providing a high level of customer service by effectively interacting with the public, vendors, students, and College staff, including individuals of various ages, disabilities, socio-economic levels and ethnic groups.

Skills & Abilities to:

1. Advocate for and communicate the College's vision and commitment to creating a diverse, equitable, inclusive, socially just, anti-racist, and accessible academic and work environment.
2. Participate in addressing gaps in diversity, equity, inclusion, social justice, anti-racism, and accessibility in the recruitment and retention of staff.
3. Participate in providing resources and support towards the goal of a diverse, equitable, inclusive, socially just, anti-racist, and accessible academic and work environment.
4. Research and maintain knowledge of best management practices for cybersecurity programs, diagnostic tools, and mitigation measures.
5. Monitor systems for security breaches, investigate incidents, and execute incident response plans to minimize impact.
6. Work independently with little to no direct supervision.
7. Establish and maintain a variety of filing, record-keeping, and tracking systems.
8. Organize and prioritize a variety of projects and multiple tasks in an effective and timely manner; organize own work, set priorities, and meet critical time deadlines.
9. Interpret, apply, explain, and ensure compliance with federal, state, and local policies, procedures, laws, and regulations.
10. Communicate effectively through various modalities.
11. Learn and apply emerging technologies and, as necessary, to perform duties in an efficient, organized, and timely manner.
12. Review situations accurately and determine appropriate course of action using judgment according to established policies and procedures; understand scope of authority in making independent decisions.
13. Establish, maintain, and foster positive and effective working relationships with those contacted in the course of work.

Education and Experience:

1. A bachelor's degree or equivalent (total units) from a regionally or nationally accredited institution with major coursework in a technical field related to computer science, cybersecurity, or information technology; and
2. Three (3) full-time equivalent years of increasingly responsible technical work experience in information technology.
   a. Full-time equivalent work experience may be substituted for years of education on a year-for-year basis.

Desirable Qualifications:

1. Possession of industry-standard certification(s) in information security, such as Certified Information Systems Security Professional (CISSP), GIAC Security Essentials (GSEC), or Cybersecurity Analyst+ (CySA+).
2. Experience working with policies and procedures relating to diversity, equity, inclusion, social justice, anti-racism, and accessibility preferably in a minority serving institution such as Hispanic Serving Institution (HSI) and Asian American and Native American Pacific Islander-Serving Institution (AANAPISI); OR
3. Experience with participation in programs relating to diversity, equity, inclusion, social justice, anti-racism, and accessibility preferably in a minority serving institution such as Hispanic Serving Institution (HSI) and Asian American and Native American Pacific Islander-Serving Institution (AANAPISI).

PHYSICAL DEMANDS

Must be able to work in a standard office setting and use standard office equipment, including technological devices; to communicate with individuals at various College and meeting sites; the ability to understand and comprehend written and electronic materials; the ability to receive, review, and respond to communications in person, before groups, and over and through various media. This is primarily a sedentary office classification, although movement between work areas may be required. Positions in this classification occasionally may need to physically reach, push, and pull drawers open and closed to retrieve and file information. Incumbents must possess the ability to lift, carry, push, and pull materials and objects weighing up to 25 pounds.

ENVIRONMENTAL ELEMENTS

Incumbents work in an office environment with moderate noise levels, controlled temperature conditions, and no direct exposure to hazardous physical substances. Incumbents may interact with staff, students, and/or the public in interpreting and enforcing departmental policies and procedures.