DEFINITION

Under the direction of the Director, Information Technology, or assigned manager, manage the development, implementation, and evaluation of Information Technology (IT) security standards, best practices, architecture, and systems to ensure the integrity and security of the District's PeopleSoft Enterprise Resource Planning (ERP) System and IT Infrastructure and the protection, integrity, and confidentiality of information assets spanning the entire enterprise.

EXAMPLE OF DUTIES

1. Develop, implement, and manage security policies, standards, and procedures for the District's PeopleSoft administrative systems, including its Finance, Human Resources Management, Campus Solutions, and Portal modules and the associated applications and services; propose and oversee policies and mechanisms to prevent the unauthorized use, disclosure, modification, loss, or destruction of data, applications, or equipment; oversee tools for managing user profiles and access rules; conduct security audits as necessary.

2. Work with central IT staff to ensure the integrity and security of the District's IT infrastructure, including data center, mainframe, virtual and dedicated servers, and other technologies; consult with application developers and other Information Technology Services staff to ensure that production applications and services meet established IT security policies and standards; review development, testing, and implementation of IT security, identity management, authentication, authorization, access control, and logging mechanisms for all departments.

3. Promote and coordinate the development of training and education on IT security and privacy awareness topics for administrators, faculty, and staff; develop appropriate security incident notification procedures.

4. Conduct vulnerability assessments to identify existing or potential electronic data and information system compromises and their sources; coordinate IT investigative matters with appropriate audit, regulatory, and law enforcement agencies.

5. Perform audits and periodic inspections of central and departmental information technologies to ensure security measures are functioning and effectively utilized; recommend appropriate remediation measures to eliminate or mitigate future system compromises.

6. Review, evaluate, and recommend software and hardware products related to IT security, such as virus and malware scanners, encryption technology, firewalls, Internet filtering and monitoring, intrusion detection, intrusion prevention, and other related products.

7. Contribute to, participate in, and support the District's IT governance groups.

8. Participate in review of systems for computer- and network-based electronic control of building access, HVAC, power, and similar functions to ensure conformity to established security policies and guidelines.

9. Serve as a witness or subject matter expert for Information Technology Services in legal matters concerning IT security.

10. Maintain up-to-date technical knowledge by attending educational workshops, reviewing professional publications, establishing personal networks, and participating in professional organizations and associations focused on information security in higher education.

11. Train, supervise, and evaluate the work performance of assigned staff; provide technical direction and guidance; recommend personnel actions, including employment, change in status, and disciplinary action.

12. Perform related duties as assigned.

DESIRABLE QUALIFICATIONS

Knowledge:

- Applicable federal and State laws, codes, and regulations.
- Current trends and advancements in enterprise-wide technology security management, including multifactor authentication and single-sign on mechanisms, security risk identification and mitigation, security architecture, and compliance.
- Oral and written communication skills.
- PeopleSoft security architecture, mechanisms, and operation.
- Principles and practices of administration, supervision, and training.
- Problem diagnosis, analysis, and resolution techniques.
- Project management principles and practices.
- Technical aspects of field of specialty.

Skills and Abilities:

- Assess IT security at the departmental and organizational levels.
- Communicate effectively both orally and in writing.
- Communicate technical information to a non-technical audience.
- Conduct timely investigations and responses to computer security-related incidents and threats.
- Coordinate activities with other internal departments and/or external agencies.
- Demonstrate interpersonal skills using tact, diplomacy, and courtesy.
- Develop, implement, and manage security policies, standards, and procedures for the District's PeopleSoft administrative systems.
- Ensure the integrity and security of the District's PeopleSoft ERP System and IT infrastructure.
- Ensure the protection, integrity, and confidentiality of information assets spanning the entire enterprise.
- Establish and maintain effective working relationships with others.
- Explain and implement security policies and measures and detect and resolve problems.
- Interpret, explain, and apply District rules, regulations, policies, and procedures.
- Manage the development, implementation, and evaluation of IT security standards, best practices, architecture, and systems.
- Meet schedules and timelines.
- Operate computers and related equipment.
- Oversee tools for managing user profiles and access rules; conduct security audits as necessary.
- Plan and organize work.
- Prepare a variety of reports.
- Promote and coordinate the development of training and education on IT security and privacy awareness topics for administrators, faculty, and staff.
- Propose and oversee policies and mechanisms to prevent the unauthorized use, disclosure, modification, loss, or destruction of data, applications, or equipment.
- Provide technical guidance to users and other technical specialists.
- Relate effectively with people from varied cultural and socio-economic backgrounds.
- Review development, testing, and implementation of IT security, identity management, authentication, authorization, access control, and logging mechanisms for all departments.
- Train, supervise, evaluate, and provide work direction and guidance to others.
- Work independently with little direction.

Training and Experience:

Any combination of training and experience equivalent to: a Bachelor's Degree in Computer Science, Information Technology, Systems Engineering, or a related field and five years of progressively responsible experience in designing, administering, implementing, monitoring, and maintaining applications and/or IT infrastructure systems, including at least two years of security program development and experience involving risk identification and mitigation and security architecture development and compliance.

WORKING CONDITIONS

Physical Requirements:

Category III: Typically sedentary in nature.

Environment:

Work is performed primarily in an office environment with a computer, monitor, keyboard, and mouse, requiring long-term viewing of computer terminal displays; may require prolonged periods of sitting.