PALOMAR COLLEGE

Classification Title: Information Technology Security Officer

Department:	Information Services	**EEO6 Code:**	3
Employee Group:	Classified	**Salary Grade:**	55
Supervision Received From:	Director, Information Services	**Date of Origin:**	9/2016
Supervision Given:	Direction and Guidance	**Last Revision:**	9/2016

Class specifications are intended to present a descriptive list of the range of duties performed by employees in the class. Specifications are not intended to reflect all duties performed by individual positions.

JOB SUMMARY.

Manages the development, implementation and evaluation of information technology (IT) security standards, best practices, architecture and systems for the District to ensure the integrity and security of the District's IT infrastructure and the protection, integrity and confidentiality of information assets spanning the entire enterprise.

DISTINGUISHING CHARACTERISTICS.

The Information Technology Security Officer is distinguished from Infrastructure Systems Engineer by the former's responsibility for managing the District's overall IT security program while the latter position focuses on designing, implementing and maintaining the District's technology infrastructure.

ESSENTIAL AND MARGINAL FUNCTION STATEMENTS.

Essential Functions: Essential responsibilities and duties may include, but are not limited to, the following:

1. Develops and implements security policies, standards and procedures intended to prevent the unauthorized use, disclosure, modification, loss or destruction of data; works with the Infrastructure Systems Engineer to ensure the integrity and security of the District's IT infrastructure; reviews the development, testing and implementation of IT security products and control techniques for all departments within the District, including academic systems, Educational Television and Telecommunications – Grants.
2. Consults with Application Developers and other Information Services staff to ensure production applications will meet established IT security policies and standards.
3. Promotes and coordinates the development of training and education on IT security and privacy awareness topics for District administrators, faculty and staff; develops appropriate security incident notification procedures for District administration.
4. Conducts vulnerability assessments to identify existing or potential electronic data and information system compromises and their sources; coordinates IT investigative matters with appropriate law enforcement agencies.
5. Performs audits and periodic inspections of departmental information technologies to ensure security measures are functioning and effectively utilized and recommends appropriate remediation measures to eliminate or mitigate future system compromises.

6. Conducts the review, evaluation and recommendation of software and hardware products related to IT security, such as virus and malware scanners, encryption technology, firewalls, Internet filtering and monitoring, intrusion detection/prevention, and other related products.
7. Contributes to and participates in supporting the District's IT governance groups.
8. May participate in the review of IT facility acquisition, construction and remodeling projects to ensure conformity to established security policies and guidelines.
9. May serve as a witness or subject matter expert for Information Services in legal matters concerning IT security.
10. Maintains up-to-date technical knowledge by attending educational workshops, reviewing professional publications, establishing personal networks and participating in professional associations.

Marginal Functions:

1. Attends various meetings and participates on committees as required.
2. Performs related duties and responsibilities as required.

QUALIFICATIONS.

Experience and Education/Training Guidelines: Any combination of experience and training that would likely provide the required knowledge and abilities is qualifying. A typical way to obtain the knowledge and abilities would be:

Experience: Five years of recent, progressively responsible experience in designing, configuring, administering, implementing, monitoring and maintaining applications and/or IT infrastructure systems, including two years of security program development and experience involving risk identification and mitigation, security architecture development and compliance.

Education/Training: Equivalent to a bachelor's degree from an accredited college or university with major coursework in computer science, information technology, systems engineering or a related field.

Knowledge of:

1. Current trends and advancements in enterprise-wide technology security management, including IT security risk identification and mitigation.
2. IT security architecture and compliance.
3. Disaster recovery planning and testing, auditing, risk analysis and business continuity planning.
4. Advanced IT security and IT audit concepts and techniques.
5. Conducting timely investigations and responses to computer security-related incidents.
6. Enterprise operating systems.
7. IT and architecture used in a college setting.
8. Open Systems Interconnection (OSI) model layer networking technologies and concepts.
9. Server virtualization technologies.

Skill in:

1. Assessing IT security at the departmental and organization levels of an institution.
2. Assisting in development of local architectures and security solutions.

3. Conducting timely investigations and responses to computer security-related incidents and threats including viruses, worms and other system compromises.
4. Providing comprehensive information security awareness and training.
5. Assisting with investigations initiated by internal and external authorities.
6. Monitoring and identifying any anomalous traffic and compromised systems on the campus networks.
7. Working with other staff to deploy anti-virus and other security-related desktop system software for organization-wide use.
8. Ensuring compliance with all federal, state and local legislation related to information security.
9. Maintaining sensitivity to and understanding of the diverse academic, socioeconomic, cultural, disability, gender identity, sexual orientation, and ethnic backgrounds of community college students, faculty, and staff.
10. Establishing and maintaining effective working relationships with those encountered in the course of work.

WORKING CONDITIONS.

Environmental Conditions: The employee works primarily in a computer environment amid noise, some dust and regular exposure to video screen, electrical and electronic equipment.

Physical Conditions: Essential and marginal functions may require physical fitness requirements necessary to perform the job functions with or without accommodation, such as the ability to sit for prolonged periods and use hands repetitively to operate computers and standard business equipment; close visual acuity to view computer screens.

TERMS OF EMPLOYMENT.

The duration of any fully restricted funded position in this classification is dependent upon the continuation of funding.