ANTELOPE VALLEY COMMUNITY COLLEGE DISTRICT

SYSTEM SECURITY ADMINISTRATOR RANGE: 28

BASIC FUNCTION:

Under the direction of the Director of Information Technology Services, design and coordinate application, systems, network, internet, and intranet security activities including but not limited to routing, firewall and switch management, user credential and authentication management and physical equipment security. Incumbent will work closely with the Network Manager, Computer Systems Manager and all levels of ITS employees to ensure consistent, robust and redundant security features and functions and the critical security of the District's network, application systems, and any electronically stored data, information and configurations. Duties include participation in the development and maintenance of security standards and implementation, security policies, security education and awareness initiatives as well as business continuity and disaster recovery planning. Coordination is also required with the Risk Management department on all appropriate security initiatives. Incumbent generates a variety of reports; trains, supervises and evaluates any assigned personnel. Performs other related responsibilities as may be assigned.

REPRESENTATIVE DUTIES: E = indicates essential duties of the position

- Develop and implement a district wide IT security plan to ensure the integrity and confidentiality of electronically stored information and electronic transactions including telecommunications transactions. (E)
- Establish, maintain, and monitor all user authentication and access rules, defining specific access to network resources, files, applications, systems, services and equipment. Review, coordinate, set up and maintain user accounts including user e-mail, intranet, application and network resource access as assigned. (E)
- Evaluate system security requirements and recommend improvements to the network, application and telecommunications systems; working with other ITS personnel to design and implement approved enhancements. Help define overall network and data security strategies and procedures. (E)
- Prepare and maintain a variety of records and reports related to system security, including configuration reports; advise and assist users in proper security procedures; assist with resolving system security problems. (E)
- Prepare documentation of system security configurations, procedures and settings. (E)
- Stay abreast of legislative requirements surrounding systems security and data protection, and advise the District regarding policy, procedures and practices affecting adherence to such legislation.
- Develop, implement and manage framework for identifying, prioritizing and addressing applicable Federal, State and other legal compliance requirements.
- Participate in strategic technology planning with focus on ensuring security and access capabilities to support current and emerging technologies and protocols related to enhanced instruction, distance education, student services and administrative and operational system needs. Includes consideration of technologies such as wireless access, netcasting/podcasting, internet programming and e-commerce. (E)
- Integrate network and system design with security initiatives including network enhancements, encryption, firewall, VPN and DMZ infrastructure and authentication management. Develop, implement and manage framework for identifying location, type, and sensitivity, access requirements for all data residing anywhere within IT infrastructure. (E)
- Work closely with the Web Administrator and Network Manager to develop and document strategies to mitigate network attacks and breaches including but not limited to DOS, network intrusion, worm attacks, network spoofing, and spam/phishing. (E)
- Communicate and coordinate closely with Information Technology Services management team and employees regarding security-related issues, practices and policies. Develop, implement, maintain and oversee enforcement of IT security related policies and procedures. Develop, implement and manage district wide IT security incident response processes and procedures. (E)

SYSTEM SECURITY ADMINISTRATOR (CONTINUE)

REPRESENTATIVE DUTIES:

- Develop, implement and manage an institution wide IT security vulnerability scanning framework for the purposes of identifying IT security vulnerabilities. Coordinate periodic district wide IT security audit. Monitor and evaluate the efficiency and effectiveness of security processes and procedures and recommend and implement appropriate additions, changes, updates and revisions. Implement security and network management systems to track and monitor network traffic to identify and report on network attacks, potential network disruptions and identify network anomalies which should generate alerts and response. Coordinate with College Internet Service Provider (CENIC) as required. (E)
- In collaboration with the Information Technology Services management team, design and implement disaster recovery and business continuity plans, as well as new security configurations to protect data and system resources. (E)
- Advise management of risk issues that are related to information and data security issues and recommend actions in support of the College's wider risk management programs. (E)
- Continually analyze existing network and systems access; make recommendations for short and long term design and updates to ensure service redundancy and security.
- Develop, implement and manage a district wide IT security awareness program for employees and students.
- Develop, monitor, and maintain time lines for assigned security projects.
- Stay abreast of emerging and state-of-the-art network design and software application management security tools/technologies; provide timely recommendations to the Information Technology Services management team regarding such tools/technologies.
- Perform other related responsibilities as may be assigned.

EDUCATION AND EXPERIENCE:

Any combination equivalent to: Bachelor's degree and five years of increasingly responsible experience in Information Technology with three of these five years being in an Information Technology Security related capacity. Experience working in an IT or IT security capacity at a higher education institution is preferred.

KNOWLEDGE OF:

Information technology security standards as provided through certifications such as CISSP (Certified Information System Security Professional), CISM (ISACA Certified Information Security Manager) or CISA (ISACA Certified Information Security Auditor).
Computer hardware systems, software applications and network infrastructures utilized by the District.
Technical aspects of information technology security associated with Internet and network services, operations, user access and authentication, software applications and programming.
District organization, operation, policies and objectives.
Interpersonal skills using tact, patience and courtesy.

ABILITY TO:

Plan, design, install, administer and document the District's information technology security systems, procedures and utilities.
Clearly and professionally communicate security procedures and requirements to users.
Apply principles and techniques of information technology security design to meet specific District requirements.
Develop and implement information technology security policies, procedures and processes.
Review and verify network, application and data security to assure confidentiality and integrity.
Operate information technology equipment properly and efficiently.
Establish and maintain cooperative and effective working relationships with others.

CONTACTS:

Co-workers, staff, other departmental personnel, administration, contractors and vendors.

PHYSICAL EFFORT:
Dexterity of hands and fingers to operate a computer keyboard and work with network infrastructure components. Sitting for extended periods of time.

WORK DIRECTION, LEAD AND SUPERVISORY RESPONSIBILITIES:
No permanent full-time staff to supervise. However, this class, by the nature of the duties and responsibilities is required to provide technical guidance and training to other employees demonstrating work methods. May supervise temporary hourly or student employees.

WORKING CONDITIONS:
Normal office environment.