Director, IT Security
District Office
Kern Community College District
JOB DESCRIPTION

Definition

Reporting to the Chief Information Officer, the Director of IT
Security develops and implements procedures, policies, strategies and standards in the management of the district's IT Security program.

Key Accountabilities

Relative to the district's IT Security, the Director of IT Security will be held accountable for the following:

- Assessing risks, threats, technologies, architecture (25% of time)*
- Recommending improvement strategies for identified gaps (25%)
- Developing, coordinating and leading Incident Response (5%)
- Developing an IT Security Plan and Policies (5%)
- Monitoring and compliance (15%)
- Implementing an End-user education and awareness program (5%)

*This is the expected percentage of time required to perform each Key Accountability for this job. These percentages may vary over time dependent on the needs of the organization. Note, only 80% of the job's actual work time is used to assign time percentages. It is expected that 20% of the work time will be used for miscellaneous tasks.

Examples of Duties

1. Work with KCCD academic and business units to facilitate IT risk assessment and risk management processes; this includes identifying location, type, sensitivity, ownership and access requirements for data being used by KCCD

2. Monitor the external threat environment for emerging threats and advise on appropriate course of action

3. Research, identify, coordinate and play key role in the implementation of appropriate IT security systems, technology and controls including firewalls, intrusion detection/prevention and vulnerability scanners.

4. Research and disseminate amongst District Office and campus IT personnel IT security best practices and resource information.

Examples of Duties (continued)

5. Develop, implement and manage district wide IT security incident response processes and procedures

6. Develop, implement and maintain a district wide IT security plan to ensure the integrity and confidentiality of information residing in KCCD workstations, servers, mobile devices and related computer peripherals

7. Develop, implement, maintain, disseminate and oversee enforcement of IT security related policies and procedures

8. Maintain an in-depth technical documentation repository of KCCD systems, networks and core applications

9. Coordinate, report on, document and act on results of periodic (annual) district wide IT security audits

10. Develop and implement strategies for complying with applicable Federal, State and other legal compliance requirements related to IT Security.

11. Develop, implement and manage a district wide IT security awareness and training program

12. Assist with the development and implementation of business continuity and disaster recovery plans

13. Participate as a member of KCCD's IT management team in the development, prioritizing, budgeting and planning of IT security strategies and related initiatives

14. Develop and communicate current IT security posture status, IT security strategies, and progress on IT security initiatives to key organizational units executive management and KCCD's Board of Trustees

15. Collaborate with other colleges and universities to share information or resources, as necessary, and to improve overall security of the higher education sector

16. Keep current with IT security industry research and best practices related to keeping an organization's IT systems and networks appropriately secure. This includes attending conferences and training as required to maintain IT security management proficiency

17. Develop and manage relationships with IT security vendors and consultants and recommend as appropriate solutions and partnerships that would benefit KCCD in its IT security efforts

18. Serve on and chair IT Security related District committees as appropriate

19. Perform other duties as assigned

Minimum Qualifications

- Bachelor’s degree in an IT related field.
- Five years of experience in IT Networks, Systems or Security related positions.

Desired Qualifications:

- Certifications such as CISSP (Certified Information System Security Professional), CISM (ISACA Certified Information Security Manager) or CISA (ISACA Certified Information Security Auditor) are preferred.

Knowledge and Abilities

- Ability to identify, **analyze**, prioritize and communicate impact of IT security risks and exposures
- Understanding of effective IT security system and network architectures, concepts, techniques and tools
- Understanding and experience managing network and system security components such as firewalls and intrusion detection/prevention systems
- Experience in **organizing**, prioritizing, developing, implementing and communicating status on IT security strategies and projects
- Proficiency in IT security management, industry best practices and standards
- Experience developing and implementing IT security **policies** and procedures
- Experience in and knowledge of IT security auditing and monitoring
- Knowledge of and experience meeting applicable IT security related laws and regulations
- Ability to develop, **learn** and implement new concepts, technologies and methods.
- Knowledge of and exposure in developing and testing business continuity and disaster recovery plans
- Exposure to the operation of institution wide networks, systems and applications
- Ability to **follow-up and follow-through** in a coordinating role across multiple constituencies to achieve tactical and strategic goals
- Excellent analytical, **planning** and **organizational** skills

Knowledge and Abilities (continued)

- **Agility** in adapting to and thriving in a dynamic work environment including shifting of project objectives, deadlines, resources and priorities

- Ability to work effectively with administrators, faculty and staff

- Excellent oral and written communication skills

- Self-directed/driven

Working Conditions

Environment: Office

Physical Demands: Incorporated within one (1) or more of the previously mentioned essential functions of this job description are essential physical requirements. The ratings in the chart below indicate the percentage of time spent on each of the essential physical requirements.

Seldom—Less than 25 percent = 1	Often—51-75 percent = 3
Occasional—25-50 percent = 2	Very Frequent—76 percent and above = 4

Ratings	Essential Physical Requirements
4	Ability to work at a desk, conference table or in meetings of various configurations
1	Ability to stand for extended periods of time.
4	Ability to sit for extended periods of time.
4	Ability to see for purposes of reading printed matter
4	Ability to hear and understand speech at normal levels.
4	Ability to communicate so others will be able to clearly understand a normal conversation.
1	Ability to lift 10 pounds.
1	Ability to carry 10 pounds.
4	Ability to operate office equipment.

Status/Rationale

This is a classified administrator position.

Signature/Approval

(Employee's Signature)	(Date)
(Supervisor's Signature)	(Date)