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
Occasional—25-50 percent = 2
Often—51-75 percent = 3
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)

CLASS TITLE: Security Engineer

BASIC FUNCTION:

Under the direction of an assigned supervisor, provide technical leadership, coordination and planning in support of KCCD's IT Security systems and initiatives; and design, develop, test, install, monitor, and maintain information technology (IT) security systems for the district.

REPRESENTATIVE DUTIES:

Serve as the security engineer supporting security initiatives district-wide and advising District office and College IT staff on IT Security matters. ***E***

Coordinate with District office and College IT staff in troubleshooting and resolving IT Security related support requests in a timely manner. ***E***

Coordinate team efforts to research, select, plan, implement and support effective IT Security controls, monitoring tools and practices. ***E***

Assist with performing periodic and scheduled IT security audits, vulnerability scans and/or risk assessments to identify vulnerabilities and potential threats, and recommend mitigation practices. ***E***

Conduct assessments and implements strategies for ensuring KCCD meets IT Security compliance requirements, including those associated with FERPA, PCI, and HIPAA. ***E***

Monitor security systems and identify, troubleshoot, diagnose, resolve and report IT security problems and incidents; help coordinate and conduct investigations of suspected breaches in IT Security; respond to emergency IT security situations. ***E***

Maintain vendor contacts, partnerships, and relationships related to the implementation and support of KCCD's IT security architecture and programs. ***E***

Research, recommend and facilitate adoption of IT Security Standards for KCCD IT systems and networks (e.g. servers, routers, databases). ***E***

Monitor external IT Security threat environment for emerging threats and advise on appropriate course of action. ***E***

Develop, maintain, and present IT Security awareness training for staff and faculty. ***E***

Develop and maintain documentation for KCCD's IT Security architecture and programs. ***E***

Receive, prioritize and respond to help desk service tickets for IT Security-related issues. ***E***

Develop and maintain help desk knowledge base articles for respective areas of responsibility.

Backup other IT Security, Network and Systems team members as needed.

Keep current with the latest developments in IT Security industry.

Perform related duties as assigned.

KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:

A variety of IT and security concepts including several of the following:

- Multiple operating systems including recent desktop and server versions of Microsoft Windows and Redhat Linux or other Linux distributions.
- IT architecture including data centers, cloud deployment, containers, etc.
- Networking including routing and switching concepts, Ethernet, wireless networking, TCP/IP, and NetBIOS.
- Programming or scripting ability in at least one language such as Python, PHP or Powershell.
- Security Protocols including WPA/WPA2, Kerberos/AD, IPSEC, SSL/TLS, and SSH.
- Security assessment and scanning tools such as Nessus, Nmap, oclHashCat, Kali.
- Detection and monitoring tools including network-based IDS/IPS software and appliances, and endpoint detection and response software.
- Computer forensics and incident response tools and procedures.
- Security standards and frameworks such as NIST, PCI-DSS, OWASP, or CIS Critical Security Controls.
- Effective communication, documentation and writing skills.
- Effective customer service skills and practices.

ABILITY TO:

- Effectively interact and negotiate with vendors.
- Assess and remedy system performance problems.
- Troubleshoot and resolve complex hardware and software problems.
- Plan, organize, implement, and complete complex IT security projects.
- Work independently with little direction.
- Prepare and follow work plans and timelines for projects and tasks.
- Learn new skills and adapt to changes in technology.
- Communicate effectively, both orally and in writing.

- Establish and maintain cooperative and effective working relationships with others.

EDUCATION AND EXPERIENCE:

Any combination equivalent to:

Bachelor's degree in computer science, information technology, or a related field and three years of experience in a system administration, networking, or IT security role.

OR

Associate's degree in computer science, information technology or a related field and five years of experience in a system administration, networking, or IT security role.

OR

A high school diploma, GED or equivalent certificate of competency and seven years of experience in a system administration, networking, or IT security role.

Preferred: One or more relevant technical security certifications such as the CCNA: Security, Offensive Security Certified Professional (OSCP), or a SANS certification. At least two years of experience in an IT security role.

WORKING CONDITIONS:

ENVIRONMENT:
Office environment.
Driving a vehicle to conduct work

PHYSICAL DEMANDS:
Incorporated within one or more of the previously mentioned essential functions of this job description are essential physical requirements. The chart below indicates the percentage of time spent on each of the following essential physical requirements.

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

4 a. Ability to work at a desk, conference table or in meetings of various configurations.
2 b. Ability to stand for extended periods of time.
4 c. Ability to sit for extended periods of time.
4 d. Ability to see for purposes of reading printed matter.
2 e. Ability to hear and understand speech at normal levels.
4 f. Ability to communicate so others will be able to clearly understand a normal conversation.
2 g. Ability to bend and twist.
2 h. Ability to lift 25 lbs.

2 i. Ability to carry 25 lbs.
4 j. Ability to operate office equipment, computer or related peripherals.
3 k. Ability to reach in all directions.

This job description is intended to describe the general nature and level of work being performed. It is not intended to be construed as an exhaustive list of all responsibilities, duties and skills required of individuals so classified.

CLASS TITLE: Security Specialist

BASIC FUNCTION:

Under the direction of an assigned supervisor, provide support for District's IT Security systems and initiatives; and evaluate, test, install, monitor, and maintain information technology (IT) security systems for the district.

REPRESENTATIVE DUTIES:

Support security initiatives district-wide and advising District office and College IT staff on IT Security matters. *E*

Coordinate with District office and College IT staff in troubleshooting and resolving IT Security related support requests in a timely manner. *E*

Participate in team efforts to research, select, plan, implement and support effective IT Security controls, monitoring tools and practices. *E*

Responsible for the maintenance and support of system related to account provisioning, single sign-on and identity management. *E*

Assist with performing periodic and scheduled IT security audits, vulnerability scans and/or risk assessments to identify vulnerabilities and potential threats, and recommend mitigation practices. *E*

Help implement and assess compliance with IT security standards, including those associated with FERPA, PCI, and HIPAA. *E*

Monitor security systems and identify, troubleshoot, diagnose, resolve and report IT security problems and incidents; help conduct investigations of suspected breaches in IT Security; respond to emergency IT security situations. *E*

Maintain vendor contacts, partnerships, and relationships related to the implementation and support of KCCD's IT security architecture and programs. *E*

Research, recommend and facilitate adoption of IT Security Standards for District IT systems and networks (e.g. servers, routers, databases). *E*

Maintain, and present IT Security awareness training for staff and faculty. *E*

Develop and maintain documentation for District's IT Security architecture and programs. *E*

Receive, prioritize and respond to help desk service tickets for IT Security-related issues. *E*

Develop and maintain help desk knowledge base articles for respective areas of responsibility. *E*

Backup other IT Security, Network and Systems team members as needed. *E*

Keep current with the latest developments in IT Security industry. *E*

REPRESENTATIVE DUTIES (Continued):

Perform related duties as assigned.

KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:
A variety of IT and security concepts including several of the following:

- Multiple operating systems including recent desktop and server versions of Microsoft Windows and Redhat Linux or other Linux distributions.
- IT architecture including data centers, cloud deployment, containers, etc.
- Networking including routing and switching concepts, Ethernet, wireless networking, TCP/IP, and NetBIOS.
- Programming or scripting ability in at least one language such as Python, PHP or Powershell.
- Security Protocols including WPA/WPA2, Kerberos/AD, IPSEC, SSL/TLS, and SSH.
- Security assessment and scanning tools such as Nessus, Nmap, oclHashCat, Kali.
- Detection and monitoring tools including network-based IDS/IPS software and appliances, and endpoint detection and response software.
- Computer forensics and incident response tools and procedures.
- Security standards and frameworks such as NIST, PCI-DSS, OWASP, or CIS Critical Security Controls.
- Effective communication, documentation and writing skills.
- Effective customer service skills and practices.

ABILITY TO:

- Effectively interact and negotiate with vendors.
- Assess and remedy system performance problems.
- Troubleshoot and resolve complex hardware and software problems.
- Plan, organize, implement, and complete complex IT security projects.
- Work independently with little direction.
- Prepare and follow work plans and timelines for projects and tasks.
- Learn new skills and adapt to changes in technology.
- Communicate effectively, both orally and in writing.
- Establish and maintain cooperative and effective working relationships with others.

EDUCATION AND EXPERIENCE:

Any combination equivalent to:

Bachelor's degree in computer science, information technology, or a related field and two years of experience in a system administration, networking, or IT security role.

OR

EDUCATION AND EXPERIENCE (Continued):

Associate degree in computer science, information technology or a related field and four years of experience in a system administration, networking, or IT security role.

OR

A high school diploma, GED or equivalent certificate of competency and six years of experience in a system administration, networking, or IT security role.

Preferred: One or more relevant technical security certifications such as the CCNA: Security, Offensive Security Certified Professional (OSCP), or a SANS certification. Previous experience in an IT security role.

WORKING CONDITIONS:

ENVIRONMENT:
Office environment.
Driving a vehicle to conduct work

PHYSICAL DEMANDS:
Incorporated within one or more of the previously mentioned essential functions of this job description are essential physical requirements. The chart below indicates the percentage of time spent on each of the following essential physical requirements.

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

4 a. Ability to work at a desk, conference table or in meetings of various configurations.
2 b. Ability to stand for extended periods of time.
4 c. Ability to sit for extended periods of time.
4 d. Ability to see for purposes of reading printed matter.
2 e. Ability to hear and understand speech at normal levels.
4 f. Ability to communicate so others will be able to clearly understand a normal conversation.
2 g. Ability to bend and twist.
2 h. Ability to lift 25 lbs.
2 i. Ability to carry 25 lbs.
4 j. Ability to operate office equipment, computer or related peripherals.
3 k. Ability to reach in all directions.

This job description is intended to describe the general nature and level of work being performed. It is not intended to be construed as an exhaustive list of all responsibilities, duties and skills required of individuals so classified.

INFORMATION TECHNOLOGY

Welcome to our Kern Community College District Information Technology (IT) web page.

The primary mission of Information Technology (IT) is to provide students, faculty, and staff high quality technology solutions, support, and innovation in the delivery of information technology products and services supporting the education of our students. We provide a transparent and collaborative environment for technology discussion, direction, and information encouraging district-wide collaboration and communications by working though IT on technology issues.

We are aggressively working to transform ourselves into an exemplary, agile technology support and development organization utilizing the exceptional technologists in IT. We measure our success by the success of our clients.

Please submit comments to our IT management team: **itfeedback@kccd.edu**.

If you have an IT related problem or need to report an outage, contact the DO IT Help Desk at x5197 or visit **support.kccd.edu**. The Help Desk staff will log your call and if they are unable to resolve your issue, will route it to the appropriate DO IT staff member.

Department Supervisor

Department Assistant

Cynthia Munoz,
Administrative Assistant

(661) 336-5147

Contact Information

- **Location:** District Office
- **Phone:** (661) 336-5147
- **Fax:** (661) 336-5196

Gary Moser

Chief Information Officer

Department Directory

Vice Chancellor

Name	Position	Phone	Location
Gary Moser	Chief Information Officer	(661) 336-5147	212A
David Barnett	Deputy Chief Information Officer	(661) 336-5157	212I

Administrative Assistant

Name	Position	Phone	Location
Cynthia Munoz	Administrative Assistant	(661) 336-5147	212

Name	Position	Phone	Location
Mayra Reyes Bonilla	Department Assistant III	(661) 336-5143	212

Project Management

Name	Position	Phone	Location
Danielle Hillard-Adams	Enterprise IT Project Manager	(661) 336-5020	212C

Infastructure

Name	Position	Phone	Location
Eddie Alvarado	Director, IT Infrastructure	(661) 336-5137	212G
Hernando Mondragon	IT Customer Support Operations Manager	(661) 336-5033	212N
Michael Arnold	Cloud Infrastructure Engineer	(661) 336-5195	212H
Juan Lucero	Senior Network Engineer	(661) 336-5159	212H
Justin Kelley	Network Engineer	(661) 336-5166	212H

Name	Position	Phone	Location
Jeremy Horton	Network Engineer	(661) 336-5194	212H
Zachary Perigo	Network Engineer	(661) 336-5160	212H
Suyun Ding	Senior Systems Administrator	(661) 336-5120	212F
Dana Tusaw	Systems Administrator	(661) 336-5191	212F
Justin Wallace	Systems Administrator	(661) 336-5163	212F
Armando Martinez	Systems Administrator	(661) 336-5167	212F
Felishia Roel	Systems Support Specialist I	(661) 336-5163	212N

Enterprise Applications

Name	Position	Phone	Location
Stephen Kegley	Director, Enterprise Applications	(661) 336-5144	212K
Daniel Chavarria	Associate Director, Enterprise Applications	(661) 336-5125	212J

Name	Position	Phone	Location
Brian Tully	ERP Analyst II	(661) 336-5098	212D
William Michal	ERP Analyst II	(661) 336-5126	212E
Juzar Roopawala	ERP Analyst I	(661) 336-5148	212D
Michael Raboy	ERP Analyst I	(661) 336-5152	212J
Sabrina Smith	ERP Analyst I		
Alvin Bunk	ERP Analyst I	(661) 336-5018	212J
Candy Carrizales	ERP Analyst I	(661) 336-5061	212J
Max Michelon	ERP Analyst I		
Diego Mendiola	Systems Support Analyst		
Joseph White	Cloud Application Engineer	(661) 336-5172	212H
Dylan Cavazos	Business Analyst	(661) 336-5123	

Security

Name	Position	Phone	Location
Lee Ann Herron	Director, IT Security	(661) 336-5111	212G
Patrick Ferree	Security Engineer	(661) 336-5187	212F
Marco Galvez	Security Specialist	(661) 336-5149	212D