Position Information

Title	**Director, IT Infrastructure and Security**
Job Category	Management
Position Number	
Location	
Job Description	BASIC FUNCTION: The Director of IT Infrastructure & Security (DIIS) is a critical member of the Chief Technology Officer's (CTO's) team. The DIIS is a leadership role and is an empowered representative of the CTO and acts as the Information Security Officer for Yuba Community College District. This position requires an individual with a strong technical background, as well as an ability to work across all district constituencies to align priorities and plans with key business objectives. The Director provides strategic direction for the organization's technical infrastructure and security (including hardware, software, servers, databases, storage solutions, networks, audiovisual equipment or physical facilities) in support of critical district business needs.
Job Duties	DESCRIPTION OF RESPONSIBILITIES WILL INCLUDE BUT NOT BE LIMITED TO THE FOLLOWING: 1. Leadership a. Provides leadership, motivation, coaching, professional development and day-to-day support to foster an engaged work environment with a focus on customer service. b. The Director will oversee the selection, development, deployment, monitoring, maintenance, and enhancement of the district's technology infrastructure. c. Assists staff in developing methods and processes to improve the effectiveness, efficiency and security of the network services, desktop support and user support functions. d. Stays current in technology trends and proactively provides technology recommendations. e. Will serve as a liaison including developing and maintaining relationships with local school districts and government agencies. f. Establishes service level agreements and monitors progress toward key service delivery performance indicators (KPI's) or metrics. g. Manages the development and delivery of IT standards, best practices, architecture and systems to ensure information system security across the enterprise. h. Ensure that appropriate communications take place throughout the location(s) by facilitating/participating in monthly open-book meetings, conducting regular team meetings, encouraging an open-door policy, and proactively seeking feedback from team members. 2. Operations a. Manages the daily operations of the Enterprise Hardware Group (networking, desktop support, audiovisual technicians) and IT Service Desk (service desk, trainers). b. This position will directly and indirectly manage exempt employees and actively influence (faculty and staff) leadership throughout the district to assure the successful implementation of district initiatives. c. Implements and maintains all network services infrastructure with special emphasis on the security and stability of Yuba Community College District systems and their confidential data.

d. Manages and participates in the planning and implementation of security standards, practices and procedures to ensure system security and legal compliance.

e. Manage vendor relationships ensuring that service levels and vendor obligations are met.

f. Develop, schedule, test and communicate the IT Disaster Recovery plan and Procedures.

g. Collaborate with the CTO on the evaluation, allocation, and management of physical and financial resources and administer the hiring, development/training, management, evaluation, and effective assignment of personnel.

h. Architect appropriate technological, procedural, and educational/training security practices that result in an appropriate level of information security for YCCD.

i. Works collaboratively with district leadership to develop and deliver a program to educate administrators, faculty, and staff about security and compliance with regulations such as HIPAA, PCI-DSS, FERPA, et.al.

j. Partner with all departments across the district to integrate security into operational processes. (e.g., Outside Counsel, Risk Management, Human Resources, etc.)

3. Project Management

a. Provide guidance and counsel to the CTO and key members of the district leadership team, working closely with the campus community in defining objectives for enterprise hardware technology initiatives, while building relationships and goodwill through continuous communication.

b. Responsible for relationship building, creative problem solving, and proficient management of projects, resources, and new technologies in a dynamic environment.

c. Develop and maintain multiple project plans; define scope and objectives for technology initiatives.

d. Prioritizes work efforts to balance operational tasks with long-term strategic initiatives.

4. Information Security - Monitoring - Perform IT risk assessments, audits, and security incident investigations

a. Perform detailed analysis of the IT Security requirements and current state.

b. Uses methods and tools to conduct vulnerability assessments, testing internal and external network perimeters for accessibility.

c. Works with internal and external auditors to ensure compliance with adopted IT policy and procedures, and legislation related to data privacy or security provisions in safeguarding specific information.

d. Facilitates migration of non-compliant environments to compliant environments based on legal requirements, audit findings and risk assessment recommendations.

Knowledge Of:

1. Compliance, disaster recovery planning and testing, auditing, risk management, business resumption planning, and contingency planning is important.

2. Secure and effective access controls, authentication, password management, DNS, cryptography fundamentals, ICMP, IPv6, public key infrastructure, Linux, Windows servers, VMWare, SCCM, network mapping, and network protocols.

3. Technologies that support a strong security posture for a complex infrastructure.

4. Information security standards (e.g., NIST, ISO, OWASP, etc.), rules and regulations related to information security and confidentiality (e.g., PCI, HIPAA, FERPA, GLBA, 508 etc.) and other various security standards and policies.

5. A proven track record in developing information security policies, privacy policies, and procedures, and successful execution

6. Extensive knowledge of business risk, risk assessment and risk-based decision making

	7. Technical acumen including but not limited to: OSI, IT infrastructure, cloud, application development languages, tools and frameworks, database technologies, web technologies, next gen mobile, network architecture, enterprise architecture, and directory services 8. Security technology acumen and experience including but not limited to: firewall, intrusion detection, cyber-attack tools and defenses, encryption, certificate authority, web filtering, anti-malware, anti-phishing, identity and access management, multi factor authentication. Ability To: 1. Provide leadership and judgement, and to collaborate with other leaders in establishing district priorities. 2. Ability to inspire and motivate cross-functional, interdisciplinary teams to achieve tactical and strategic goals; an innovative leader, problem solver and consultant 3. Demonstrate strong interpersonal, presentation, oral communication skills, written communication skills with a strong customer service orientation and strong understanding of business processes. Knowledge, Skills and Abilities 4. Be a consensus builder and persuasive leader with a strong commitment to teamwork and knowledge sharing who effectively communicates technical concepts to a broad range of technical and non-technical staff. 5. Balance operational tasks with long-term strategic technology and security initiatives. 6. Able to communicate security and risk-related concepts to both technical and non-technical audiences (in business terms), including board level 7. A natural influencer and coalition builder; passionate about building high performing teams 8. Ability to evangelize IT security to make it a critical part of business operations; build trust and respect for the security function 9. Experienced with contract and vendor negotiations. 10. Ability to effectively prioritize and execute tasks in high-pressure situations.
Required Qualifications	MINIMUM QUALIFICATIONS: The successful candidate, by the final filing date, must possess the minimum qualifications for Educational Administrators at California Community Colleges: 1. Bachelors degree in management information systems, computer science or closely related field plus 7 years of experience. Combination of experience and education will be considered. 2. Experience in controlling information technology budget 3. Experience in analysis, implementation and evaluation of IT systems and their specifications 4. Outstanding communication abilities
Desired/Preferred Qualifications	1. Experience in managing a comprehensive enterprise-wide information security and IT risk management programs for an institution of higher education. 2. CISSP, CISM, CISA, GIAC, or other security certification/accreditation strongly preferred. 3. Participation in local and national information security working/interest groups a plus.
Physical Demands	

Special Conditions for Eligibility	
FLSA	Exempt
Range/Step	Range 40, Management Salary Schedule
Salary	$116,829- $128,946 Per Year
Benefits Information	BENEFITS/SALARY: The District offers a comprehensive benefits package for employees and dependent(s), for positions whose FTE is .60 or higher, valued at over $24,000 annually. The package includes health, dental, vision, two (2) life insurance policies and an Employee Assistance program. Additional benefits include contributions to the State Teacher's Retirement System (STRS), 457/403b options, 12 sick days, 22 vacation days, 223 day/12 month contract. FOREIGN TRANSCRIPTS: Include a U.S. evaluation and translation. Contact the Human Resources website for a list of agencies providing foreign transcript services. PRE-EMPLOYMENT REQUIREMENTS: Employment is dependent upon Department of Justice (DOJ) clearance; all fees are the responsibility of the selected candidates and serves the purpose of obtaining a criminal history as authorized by the California Education Code. All prospective employees shall be required to provide verification of TB test. WORKING CONDITIONS: In accordance to Board Policy, smoking is restricted in many areas of the Yuba Community College District. Woodland Community College is a tobacco free campus. WORK DAY, WORK WEEK, and WORK YEAR: The District has the right to establish work day, work week, work year; hours of positions within the District may vary.
EEO Statement	As an equal opportunity employer with a diverse staff and student population, the Yuba Community College District is committed to creating an inclusive and effective learning and working environment for all. EQUAL EMPLOYMENT: Yuba Community College District is an Equal Employment Opportunity Employer and guarantees equal opportunity regardless of race, color, creed, national origin, ancestry, gender, marital status, disability, religious or political affiliation, age or sexual orientation and does not discriminate in its educational programs, in employment nor in any other of its activities.