



NORTH ORANGE COUNTY
COMMUNITY COLLEGE DISTRICT



Job Description

Job Title:	Chief Information Security Officer	Salary Range:	35
Date Revised:	4/2/2026	Date Approved:	6/23/2026

PRIMARY PURPOSE

Under the general direction of an administrator, the Chief Information Security Officer (CISO) provides strategic vision, leadership, and management of the District's information security, governance, and compliance programs. The CISO is responsible for developing, implementing, and maintaining a comprehensive cybersecurity framework that protects institutional data, systems, and infrastructure across all campuses and operations.

The Chief Information Security Officer leads the design and enforcement of security architectures, policies, and protocols that ensure the confidentiality, integrity, and availability of District information assets. The CISO manages vulnerability assessments, incident response, risk mitigation, data governance, and business continuity initiatives, ensuring compliance with federal and state regulations such as FERPA, GLBA, HIPAA, and PCI-DSS.

Serving as the District's primary cybersecurity leader and advisor, the CISO fosters collaboration among campus IT departments, executive administrators, and external partners to build a security-conscious culture and safeguard the District's digital ecosystem.

DISTINGUISHING CHARACTERISTICS

The Chief Information Security Officer is distinguished by its executive-level scope and District-wide accountability for cybersecurity strategy, governance, and operational resilience.

Unlike IT Directors focused on infrastructure or application services, the CISO provides cross-functional oversight of enterprise security operations, risk management, and compliance programs, the CISO requires a blend of technical expertise and executive leadership, integrating strategic planning, policy development, and operational execution.

The Chief Information Security Officer serves as both a strategic architect and operational leader, directing information security initiatives across multiple campuses and ensuring that cybersecurity principles align with institutional goals, resource priorities, and regulatory mandates.

ESSENTIAL FUNCTIONS

Examples of essential functions are descriptive and not restrictive in nature.

Strategic Leadership and Governance

1. Provides districtwide leadership in information security strategy, governance, and policy development to ensure the protection of institutional data and technology assets.
2. Develops, implements, and maintains a comprehensive cybersecurity framework aligned with NIST, ISO, and higher education security standards.
3. Serves as the District's principal advisor on security posture, risk mitigation, and compliance.



Job Description

4. Establishes and maintains cross-departmental governance structures to ensure shared accountability for information security.

Risk Management and Compliance

5. Directs and oversees risk assessments, security audits, and compliance evaluations to identify vulnerabilities and ensure adherence to institutional, state, and federal standards.
6. Oversees data governance policies, classification frameworks, and access control procedures to safeguard personally identifiable information (PII) and other sensitive data.
7. Ensures compliance with applicable regulations, including FERPA, GLBA, HIPAA, PCI-DSS, and California data privacy laws.
8. Reviews vendor security practices, negotiates risk provisions, and ensures contractual adherence to cybersecurity standards.

Security Architecture and Operations

9. Leads the design, implementation, and maintenance of security technologies, including intrusion detection, endpoint protection, firewalls, identity and access management, and SIEM platforms.
10. Establishes and enforces architectural standards for both on-premises and cloud systems to ensure consistent security controls across environments.
11. Collaborates with IT infrastructure and application teams to integrate secure design principles throughout system and software lifecycles.
12. Directs patch management, vulnerability remediation, and configuration management across all institutional systems.

Incident Response and Business Continuity

13. Develops and maintains the District's cybersecurity incident response and disaster recovery plans.
14. Leads investigations of security events and breaches, coordinating with law enforcement, insurers, and legal counsel when necessary.
15. Conducts post-incident reviews and integrates lessons learned into updated processes and controls.
16. Oversees continuity planning and testing to minimize disruption of critical operations and data recovery time objectives (RTO/RPO).

Data Governance and Privacy Oversight

17. Implements and enforces data governance policies and data classification standards.
18. Partners with academic and administrative leaders to ensure responsible handling, storage, and sharing of data across systems.
19. Monitors compliance with privacy regulations and works closely with internal auditors and compliance officers on reporting and remediation activities.

Leadership, Supervision, and Collaboration

20. Provides direction, mentorship, and evaluation for information security staff and cross-functional teams.



Job Description

- 21. Collaborates with campus IT departments, district administrators, and faculty committees to align technology initiatives with institutional priorities.
- 22. Serves as the primary security liaison to external organizations, agencies, and professional networks.
- 23. Fosters an inclusive and proactive work culture emphasizing accountability, innovation, and continuous improvement.

Budget, Vendor Management, and Procurement

- 24. Develops and manages budgets for information security operations and initiatives.
- 25. Oversees vendor relationships and contracts for monitoring, auditing, and penetration testing services.
- 26. Evaluates new technologies and third-party solutions to enhance the District's security posture and operational efficiency.

Professional Development and Institutional Engagement

- 27. Keeps abreast of emerging threats, technologies, and regulatory changes in cybersecurity and higher education.
- 28. Represents the District at professional organizations, conferences, and security consortiums.
- 29. Promotes District-wide awareness of cybersecurity through training, workshops, and communication campaigns.
- 30. Supports accessibility and inclusion goals by developing accessible, equitable, and culturally responsive technology environments.

Technology and Process Improvement

- 31. Monitors industry trends and benchmarks to identify opportunities for continuous improvement.
- 32. innovation, sustainability, and equitable access to technology resources throughout the District and campus sites.
- 33. Learns and applies emerging technologies and software applications as needed to perform duties efficiently, effectively, and in a timely manner.

Diversity, Equity, and Inclusion

- 34. Promotes equity-minded technology planning and ensures accessibility for all users.
- 35. Participates in District/College efforts to increase the diversity of faculty and staff and to address student achievement gaps; actively assists in the creation of a welcoming and inclusive work and educational environment; attends and participates in diversity, equity, and inclusion trainings and events.

General

- 36. Performs other duties that support the overall objective of the position.



Job Description

WORKING RELATIONSHIPS

The incumbent engages and maintains contact with various District administrators, management, faculty, staff, students, vendors, government agencies and organizations, higher education institutions, the California State Chancellor's Office, and the public.

MINIMUM QUALIFICATIONS

Education and Experience:

- Master's Degree from a regionally accredited institution in Cybersecurity, Information Systems, Computer Science, or related discipline; **AND**
- Eight (8) years of progressively responsible experience in information security management; **WITH**
- Three (3) years of supervisory or management experience; **AND**
- Demonstrated success leading large-scale technology operations or transformations in a complex, multi-campus organization; **AND**
- ***Or, any combination of education and experience which would provide the required equivalent qualifications of the position.***
- Commitment to diversity. All applicants must have demonstrated sensitivity to and understanding of the diverse academic, socioeconomic, cultural, disability, gender, gender identity, sexual orientation, and ethnic backgrounds of community college students, faculty, and staff. The applicant must be able to demonstrate how their experience with these factors relates to successfully achieving the goals of the position.

DESIRABLE QUALIFICATIONS

- Professional Certifications in IT management, cybersecurity, or project management:
 - CompTIA Security +
 - Systems Security Certified Practitioner (SSCP)
 - GIAC Security Essentials Certification GSEC
 - Certified Information Systems Security Professional (CISSP)
 - Certified Information Security Manager (CISM)
 - Certified Cloud Security Professional (CCSP)
 - Certified Information Systems Auditor (CISA)
 - Certified Information Systems Security Professional (CISSP)
 - Experience leading enterprise security programs in a higher education environment.
- Demonstrated experience fostering an inclusive and welcoming work or educational environment through equity-minded approaches in professional interactions with colleagues and students.

KNOWLEDGE, SKILLS, AND ABILITIES

Knowledge:

- Knowledge and understanding of District, college, division, department, and/or program organizations, operations, policies, procedures, rules, laws, regulations, goals, and objectives related to the area of assignment.



Job Description

- Knowledge of and familiarity with the California Education Code, Title 5, and other applicable laws and regulations related to the area of assignment.
- Knowledge of Cybersecurity frameworks (NIST, ISO 27001, CIS Controls).
- Knowledge and understanding of cloud security, identity management, and network defense.
- Knowledge of network technologies, including routing, switching, DNS, DHCP.
- Knowledge of cryptography (basic concepts, algorithms, deployment, and application).
- Knowledge of cloud technologies including Azure, MS 365, CASBs.
- Knowledge of Linux fundamentals, hardening, and securing.
- Knowledge of compliance issues and industry standards frameworks.
- Knowledge of managing, crafting, and delivering complex security solutions.
- Knowledge of disaster recovery and business continuity planning.
- Knowledge and understanding of shared governance, compliance, and best practices in the public sector or higher education environment.
- Knowledge of enterprise systems, database management, network architecture, and cloud environments.
- Knowledge of enterprise IT infrastructure, systems integration, and network administration.
- Knowledge of cloud-based platforms such as Microsoft 365, Azure, and AWS.
- Knowledge of current and emerging technologies, trends, and best practices in Information Technology.
- Knowledge of budget and resource allocation management.
- Knowledge of principles and practices of supervision and training.
- Knowledge of research methods and techniques.
- Knowledge of federal and state regulations related to student services, such as FERPA.
- Knowledge of student information systems, management information systems, databases, and data management practices.
- Knowledge and awareness of equity and inclusion principles, particularly in the context of student support services.
- General knowledge of community college structures, processes, and student demographics.

Skills:

- Cybersecurity frameworks.
- Project management.
- Collaboration skills to engage technical and non-technical stakeholders.
- Strong problem-solving, analytical, and critical thinking skills.
- Strong organizational skills with the ability to prioritize and manage multiple tasks efficiently.
- Proficiency in Microsoft Office Suite (Word, Excel, PowerPoint, Outlook) and other relevant software applications.
- Excellent written and verbal communication skills, with the ability to draft clear and concise reports, correspondence, and presentations.
- Data collection, analysis, and reporting, particularly in relation to program outcomes and student participation.



Job Description

- Computer software programs, applications, databases, and Enterprise Resource Planning Systems (ERP) systems; computer hardware and peripheral equipment related to the area of assignment.

Abilities:

- Ability to independently perform the essential responsibilities of the position.
- Ability to work independently and collaboratively within a team environment.
- Ability to interact positively and professionally with a diverse student population, faculty, and staff.
- Ability to lead and present to large groups to communicate security best practices.
- Ability to drive issues to resolution across a diverse, multi-campus District.
- Ability to communicate complicated technical issues and the risks they pose to stakeholders and management.
- Ability to manage, develop, and maintain reporting systems and procedures.
- Ability to coordinate, develop, implement, and manage projects.
- Ability to direct the maintenance of a variety of reports, records, and files related to assigned activities.
- Ability to lead and inspire teams in a dynamic environment.
- Ability to analyze complex technical and operational issues and implement effective solutions.
- Ability to adapt to changing technologies and environments.
- Ability to demonstrate strong organizational and time management skills.
- Ability to analyze situations accurately and adopt an effective course of action.
- Ability to collaborate with internal and external stakeholders and colleagues.
- Ability to prepare, implement, and present training programs and workshops.
- Ability to accurately document workflow.
- Ability to compile, organize, and present statistical and technical data.
- Ability to create, write, and deliver curriculum and training materials
- Ability to lead multidisciplinary teams, prioritize initiatives, and manage multiple complex projects.
- Ability to write and update technical documentation.
- Ability to comprehend and execute both written and verbal instructions.
- Ability to prepare clear, concise, and comprehensive specifications, reports, studies, documentation, and other written materials.
- Ability to communicate efficiently, including technical information to non-technical stakeholders.
- Ability to maintain confidentiality and ethical standards in data management.
- Ability to remain current with developments in legal requirements and regulations related to the area of the assignment.
- Ability to maintain confidentiality and handle sensitive information with discretion.
- Ability to plan, organize, and prioritize workload to meet schedules and timelines.
- Ability to learn and adapt to new software, systems, and processes as required.
- Ability to provide empathetic and effective support to students, addressing their needs and concerns with professionalism.
- Ability to attend and participate in diversity, equity, and inclusion trainings and events.



Job Description

- Ability to provide an inclusive and welcoming work/educational environment.
- Ability to demonstrate a sensitivity to and understanding of the diverse academic, socioeconomic, cultural, disability, gender, gender identity, sexual orientation, and ethnic backgrounds of community college students, faculty and staff. The applicant must be able to demonstrate how their experience with these factors relates to successfully achieving the goals of the position.
- Ability to establish and maintain effective and cooperative working relationships with those encountered in the course of work.

SPECIAL REQUIREMENTS, LICENSES, and/or CERTIFICATIONS

- Possession of or ability to possess a valid driver license based on the need related to the area of assignment if and when travel is required in the course of work.
- Travel may be required for various off-site meetings, trainings, conferences, and/or events in support of the overall objective of the position.

PHYSICAL AND MENTAL DEMANDS

The physical and mental demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this class. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Physical Demands:

While performing the duties of this classification, the incumbent is regularly required to sit, walk, and/or stand, speak, or hear, both in person and by telephone. Use hands repetitively to perform fine/gross finger manipulation, handle, feel or operate standard office equipment; reach with hands and arms; and occasionally lift and carry up to 25 pounds, unassisted. Must frequently sit and/or stand for long periods of time; dexterity of hands and fingers to operate a variety of computer and office equipment. The incumbent may be required to bend at the waist, kneel, and/or crouch; move about the college or District site(s).

Specific vision abilities required by this job include close vision and the ability to adjust focus and view a variety of computer screens, printed documents, and instructions.

The incumbent may be required to work a flexible and varying work schedule based on the needs of the department, including evenings and weekends, as needed.

Mental Demands:

While performing the duties of this class, the incumbent is regularly required to use written and oral communication skills; read and interpret data, information and documents; analyze and solve problems; observe and interpret people and situations; learn and apply new information or skills; perform highly detailed work on multiple, concurrent tasks; use math/mathematical reasoning; perform highly detailed work under changing priorities and deadlines on multiple concurrent tasks; work with frequent interruptions, and interact with District and/or college faculty, staff, management, administrators, students, educational institutions, and others encountered the course of work.



NORTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT



Job Description

WORK ENVIRONMENT AND CONDITIONS

Work Environment:

The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this class. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions. The incumbent works under typical office conditions, and the noise level is usually quiet.

Working Conditions:

Work is performed primarily indoors where safety considerations exist. The incumbent may be subject to electrical hazards, constant interruptions, and frequent interaction with District and college personnel and the public. Specific vision abilities required by this job include close vision and the ability to adjust focus and view a variety of computer screens, printed documents, and instructions.

To accomplish this job successfully, an individual must be able to perform, with or without reasonable accommodation, each essential function satisfactorily. Reasonable accommodations may be made to help enable qualified individuals with disabilities to perform the essential functions of the position.

North Orange County Community College District (NOCCCD) is committed to creating a diverse academic and workforce environment that encourages and fosters diversity, equity, inclusion, and equal opportunities for everyone. NOCCCD is focused on creating a welcoming culture to ensure students, faculty, management, and staff feel included, supported, and safe.

NOCCCD looks for likeminded and inclusive individuals who represent the community's diversity and demonstrate a sensitivity to the understanding of the diverse academic, socioeconomic, cultural, disability, gender identity, sexual orientation, and ethnic backgrounds of those we represent. Our District community of professionals is devoted to enriching our students' lives by bringing a variety of ways to engage and discover their individual and collective paths through education.