**Additional Information**
June 27, 2023 Board Meeting

The following additional information was provided regarding the June 27 Board meeting agenda:

**Item 6.b, Classified Personnel, New Job Description**: Several elements of this job description don't seem correct. These minimum and desirable qualifications seem to be reversed for actually being qualified to be the CISO. The job is Chief Information Security Officer, but:

1. The minimum qualification is an advanced degree and six years of experience, but there's nothing saying either the degree or the experience has to be relevant to this specialized position. **The revised job description includes revised minimum qualifications that include experience in security or related experience.**

2. The required working security knowledge can be satisfied by knowledge of Windows and cloud technologies security only; no knowledge of such areas as incident response and data loss prevention, communication security, or defensible network design and network security is required. **The revised job description reflects changes to three or more of the bulleted items in order to be inclusive and prevent diminishing the applicant pool. This allows consideration of an applicant if they do not explicitly state all of the bulleted items on their applicant materials.**

3. A working knowledge of IT risks and having experience implementing security solutions are only desirable qualifications. **The revised job description reflects these as minimum qualifications.**

**Attached is a revised job description that was updated to note the points above. The posted agenda has been updated to reflected the revised pages.**

NORTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT
Greatness. Achieved.

# Job Description

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Position #:** | **NEW** | **Salary Range:** | **31** | **Board Approved Date:** | | **Board Revised Date:** | **N/A** |
| **Job Title: (Technical)** | Director 2, IT Security | | | **Working Title: (If any)** | Chief Information Security Officer | | |
| **Probationary Period:** | 6 Months | | | **Department/Division:** | Information Services | | |
| **Location:** | ☐ Cypress College ☐ Fullerton College ☒ District Services ☐ NOCE/Anaheim ☐ NOCE/Fullerton ☐ NOCE/Wilshire ☐ Other:_____ | | | | | | |
| **Reports to:** | Geoff Hurst, District Director, Enterprise Applications IT Support and Development | | | | | | |
| **FLSA Status:** | **Employee Group:** | | | | | | **Type of position:** |
| ☒ Exempt<br>☐ Nonexempt | ☐ Academic ☐ Classified ☐ Exec/Academic ☐ Exec/Classified<br>☐ Confidential ☐ Executive ☐ Mgmt./Academic ☒ Mgmt./Classified | | | | | | ☒ Full-Time<br>☐ Part-Time |

**Job Summary** *This job description may not be inclusive of all assigned duties, responsibilities, or aspects of the job described, and the job duties can be modified at the discretion of the Immediate Management Supervisor. The omission of specific statements of duties does not exclude them from the position if the work is similar, related, or a logical assignment to this class.*

This position is responsible for providing overall vision and leadership for the District in all areas of information security, facilitating the development and implementation of a comprehensive information security program including the design, development, deployment, and maintenance of security solutions for systems, networks, and cloud services. Conducts vulnerability management, security risk assessments, and security audits to identify, mitigate, or remediate vulnerabilities in the District's systems and networks and to meet compliance requirements with various Higher Education regulations and Cybersecurity Frameworks.

This position supports the District-wide strategic directions, goals, and core values outlined in the Educational and Facilities Master Plan (EFMP).

**Essential Job Duties and Responsibilities (percentages estimated based on comprehensive workload):**

*Information Security Leadership–*

- Provide overall vision and leadership for the District in all areas of information security, acting as a technical liaison with campus technology governance committees, working groups, and District staff in facilitating development of a comprehensive information security program.
- Develop, recommend, implement, and maintain information security policies, procedures, protocols, standards, and risk-based controls to protect the confidentiality, integrity, and availability of District data and IT systems and assets.
- Oversee and participate in risk assessment of the District's information assets and systems to identify potential threats and hazards, including assessment of the potential business impact and development of a risk management strategy aligned with the District's priorities, constraints, and risk tolerances to protect.
- Responsible for the configuration and management of various security technologies, such as intrusion detection and prevention systems, cloud security technical controls, endpoint security, privilege access and identity management, and security information and event management (SIEM) systems.
- Oversee management of user identity, authentication, and authorization controls, including limiting of access to information assets based on Data Classification policies and least privilege principles, auditing the use of privileged accounts, and enforcing the use of Multi-Factor Authentication.
- Organize, attend, or chair a variety of administrative and staff meetings as required; serve on committees and special projects as assigned; design, implement, maintain, and test disaster recovery and business continuity plans for critical District systems; oversee scheduled testing of plans.

**35%**

**REVISED PAGE**

| | |
|---|---|
| • Supervise, direct, guide, coach, train, and evaluate info rmation security staff engaged in implementing, configuring, and maintaining the District's security systems and processes. | |
| *Data Governance and Compliance –*<br>• Help oversee Data Governance frameworks, policies, and procedures; develop, implement, and monitor controls that enforce Data Classification rules and procedures; develop systems and processes for locating and securing confidential data, including Personally Identifiable Information (PII).<br>• Plan and manage the department's operating budget and program budgets for initiatives and projects.<br>• Manage relationships with vendors that provide security-related services, including monitoring, auditing, remediation, and penetration testing; direct the work of contractors and vendors as warranted. | **20%** |
| *Incident Response –*<br>• Develop and maintain security Incident Response policy, plans, and procedures for the District's critical systems; assure procedures are periodically tested and updated, utilizing metrics and evaluation criteria to assess effectiveness and continually improve response performance; engage, interact, and coordinate with third-party incident responders, including District legal counsel, cyber-insurance providers, and law enforcement; incorporate lessons learned to improve plans.<br>• Implement and maintain security monitoring systems to detect and alert for IT security issues for all technology assets; use those systems to identify, diagnose, resolve, and report IT security events and incidents; conduct incident response activities; coordinate and conduct forensic investigations of breaches in IT Security; respond to emergency IT security situations. | **15%** |
| *Risk Assessment –*<br>• Vet and review security practices and controls of third-party service providers that handle District sensitive data, including PII of students and employees; review security controls and features of third-party software systems.<br>• Conduct and direct assessments and audits to ensure District compliance to standards and regulatory requirements set forth by federal and state law or authority groups or agencies, including but not limited to FERPA, GLBA, HIPAA, and PCI-DSS.<br>• Ensure that maintenance, configuration, repair, and patching of systems occurs on a scheduled and timely basis utilizing best practices in change management and consistent with policies and procedures. | **10%** |
| *Threat Assessment -*<br>• Keep current with latest emerging security issues and threats through list servers, blogs, newsletters, conferences, user groups, and networking and collaboration with peers at other institutions. | **10%** |
| Other duties as assigned. | **10%** |

**Minimum Qualifications**

- Advanced degree from an accredited institution and at least six (6) years of experience **in Information Security** at progressively higher levels of responsibility OR an equivalent combination of education and **related** experience
- **Working knowledge of current IT risks and experience with implementing security solutions**
- CySA, SSCP, or GSEC certification; OR demonstrable working security knowledge of **three or more of** these areas:
    - Incident handling and response, data loss prevention, mobile device security, vulnerability scanning and penetration testing
    - Web communication security, virtualization and cloud security, and endpoint security
    - Defense in depth, access control and password management
    - Windows: access controls, automation, auditing, forensics, security infrastructure, and services
    - Defensible network architecture, networking and protocols, and network security
    - ~~Cloud technologies including Azure, AWS, MS 365, CASBs~~

**REVISED PAGE**

- Knowledge of one or more of these areas:
  - Network technologies including routing, switching, DNS, DHCP,
  - Cryptography: basic concepts, algorithms and deployment, and application
  - **Cloud technologies including Azure, AWS, MS 365, CASBs**
  - Linux: Fundamentals, hardening and securing

- 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**

- CISSP or CISM certification
- ~~Working knowledge of current IT risks and experience implementing security solutions~~
- Experience with Enterprise Resource Planning Systems
- Two years of professional experience involving enterprise-wide strategic technology planning and infrastructure management
- Experience in shared/participatory governance in an educational setting
- High level of critical thinking, problem solving and analytical skills
- High professional standards and strong interpersonal skills
- Effective oral and written communication skills
- Prior experience in approaching work and interactions with colleagues and/or students in an equity-minded manner. Ability to provide an inclusive and welcoming work/educational environment.

**Knowledge, Skills, and Abilities**

Knowledge of a shared governance model.
Knowledge and understanding of the diverse academic, socioeconomic, cultural, disability, gender, gender identity, sexual orientation, and ethnic backgrounds of community college students, faculty and staff.
Knowledge of compliance issues and industry standards frameworks.
Knowledge of managing, crafting and delivering complex security solutions.
Knowledge of District organization, operations, policies and objectives.
Knowledge of state education code and requirements, including Title 5.
Knowledge of applicable federal and state laws, codes, and regulations.
Knowledge of emerging IT technologies and the possible impact on existing information systems, instructional processes and business operations.
Knowledge of principles and practices of administration, supervision, and performance evaluation.
Knowledge of enterprise resource planning systems and software applications.
Knowledge of disaster recovery and business continuity planning.
Knowledge of general research techniques and data driven analytics.
Knowledge of budget development and maintenance.
Knowledge of appropriate software and databases.
Knowledge of principles of agile project management, planning and program review.
Knowledge of correct English usage, grammar, spelling, punctuation, and vocabulary.
Ability to interact with a broad cross-section of employees to explain and enforce security measures.
Ability to provide an inclusive and welcoming work/educational environment.
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 work with diverse teams in a dynamic environment.
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 encourage professional excellence among the staff and promote an organizational culture of customer service, innovation, and quality services.
Ability to lead, motivate, train, supervise, evaluate personnel and provide work direction.
Ability to assess, analyze, implement and evaluate complex project activities.
Ability to analyze situations accurately and adopt effective courses of action.
Ability to clearly organize and present information.
Ability to implement and facilitate organizational change.

| |
|---|
| Ability to maintain current knowledge of technological trends and advances in the field to provide direction for future systems and applications.<br>Ability to plan and organize work to meet changing priorities and deadlines.<br>Ability to exercise initiative and independence of judgment and action.<br>Ability to communicate efficiently orally and in writing, with internal and external diverse constituencies.<br>Ability to establish and maintain effective working relationships with others. |
| **Working Environment and Physical Demands** |
| Office environment; subject to constant interruptions and frequent interaction with others; sitting or standing for long periods at a time (up to 2-3 hours); may require off-site duties and activities. |
| **Driver's License Required** |
| ☐ Yes ☒ No |

***Acknowledgement of Receipt by Employee:***

Printed Name _____ Signature _____

Date Received _____

*Rev. 6/2023*