# PERALTA COMMUNITY COLLEGE DISTRICT – October 2024

CLASSIFIED JOB DESCRIPTION

# INFOSEC PROGRAM COORDINATOR/NETWORK COMMUNICATIONS ADMINISTRATOR

**(SEIU Local 1021 Salary Range 123)**

**Job Code: 1085**

## CLASS PURPOSE

Under the direction and supervision of the Chief Technology Information Officer for Information Technology, the position develops, organizes, plans, and coordinates the District’s information security program in a multi-college environment. The position is responsible for developing information security policies and guidelines, monitors systems to ensure compliance, enhancing the information security infrastructure, coordinating information security efforts, providing technical direction to staff, leads projects concerning the evaluation and implementation of security-related technologies, coordinating I.T. projects, and providing functional technical support within the I.T. Department. Performs related duties as required or assigned.

## EXAMPLES OF ESSENTIAL DUTIES

Any one position may not include all the duties listed nor do listed examples include all tasks that may be found in positions of this class. To perform this job successfully, an individual must be able to perform each essential duty of the position satisfactorily. Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions required for the position.

* Develops and maintains District-wide standards for information security, reviewing relevant policies and procedures; implementing strategies for complying with applicable federal, state, and other legal compliance requirements related to information security.
* Provides guidance to the District and campus community regarding relevant laws and policies.
* Research information security best practices for the District and campus community; determining how control requirements from security frameworks apply to the enterprise.
* Serves as a liaison for third-party information security auditors and assessors; translates auditing requirements for internal parties.
* Manages third-party vendor risk assessment program (TPRM); performs risk analysis of new technologies.
* Develops and maintains the District’s I.T. security incident response plan and procedures; participates in response efforts to cybersecurity incidents.
* Assists with the development and implementation of business continuity and disaster recovery plans.
* Monitors security alerts on various platforms and collaborates with IT staff to address and remediate security issues.
* Apply federal and state laws regarding data privacy and the protection of data assets.
* Maintain and monitor the usage of the Cisco VoIP, network and telecommunications systems.
* Moves, adds and changes VoIP/telecom/network communications equipment.
* Coordinates installation/repair of network communications equipment with outside vendors and contractors.
* Plan, design, implement, support, and analyze emerging IP network and telecommunications technologies.
* Participates and contributes to I.T. related District committees.
* Coordinates and directs I.T. staff on a program or project basis.
* Performs project coordination activities for the District I.T. Department.
* Reviews facilities acquisition, construction, and remodeling projects to ensure alignment to defined District I.T. standards.
* Attends workshops, conferences, and other training to maintain industry awareness and advancements as it relates to information security.
* Perform other related duties as assigned by the Chief Technology Information Officer.

## MINIMUM QUALIFICATIONS

* 1. Completion of bachelor's degree in computer information systems or closely related field, and five (5) years of experience in IT networks, systems administration, or security-related positions. An equivalent combination of education and relevant work experience may be substituted for education/experience on a year-by-year basis or equivalent combination of training & experience that could provide the desired knowledge and abilities to perform the position.
	2. Understanding of, sensitivity to, and respect for the diverse academic, socioeconomic, cultural, disability and ethnic backgrounds of Peralta Colleges’ students, faculty, staff and community.

## DESIRABLE QUALIFICATIONS

* Bachelor's degree from an accredited college or university with major course work in computer science, information science, computer information systems or a related field.
* Cisco networking communications technologies (CUCM, Unity).
* Industry recognized information security certifications: CISSP, CISM, CISA, GIAC *(preference given to candidates with an active security specific industry certification).*
* Industry recognized I.T. certifications: Cisco, Microsoft, Amazon, CompTIA.
* Experience working in a community college with diverse student and staff population.

Knowledge of:

* Information systems security architecture and compliance.
* Current trends and advancements in enterprise-wide technology security management, including IT security risk identification and mitigation.
* Working knowledge and experience with enterprise networking and telecommunications technologies.
* Knowledge of enterprise operating systems, server virtualization technologies.
* Information systems and architecture used in an educational institutional setting.
* OSI model, data networking concepts and technologies.
* Concepts and principles of security equipment, such as firewalls, access control lists, intrusion detection and intrusion preventions systems.
* Principles and theory of disaster-recovery design and planning; including audit requirements, legal requirements, risk analysis, and recovery strategies.
* Federal, state, and local regulations and guidelines related to information security: HIPAA, FERPA, FISMA, PCI-DSS and GLBA.
* Risk Management and Control Frameworks: NIST 800-53, ISO 27001, CSF, CIS.

Ability to:

* Conduct information security assessments; identify, prioritize, and communicate impact of I.T. security risks and exposures.
* Provide effective liaison among management, programmers, IT staff, auditors on information security issues and activities.
* Provide technical advice and assistance on matters relating to the installation, operation, and support of information systems including multiple networks, peripherals, telecommunications, and Internet.
* Exercise high-level problem-solving skills and follow-through on assignments.
* Work as a team in a collaborative and supportive manner.
* Multi-task several jobs at one time under sometimes stressful conditions.
* Use electronic test equipment and common small hand tools.
* Execute and communicate clear oral and written instructions.
* Comprehend technical manuals and instructions.

## ENVIRONMENTAL DEMANDS

* Occasional work performed alone.
* Constant work around and with people.
* Work schedule flexibility.

## PHYSICAL REQUIREMENTS

* Occasional standing, walking, stooping, kneeling, squatting, and climbing stairs.
* Occasional lifting and carrying up to 25 lbs.
* Occasional pushing and pulling up to 40 lbs.
* Occasional twisting of body.
* Occasional use of manual dexterity.
* Occasional use of tactile acuity.
* Occasional use of visual acuity from a distance, with depth, and for color.
* Frequent work at a rapid pace.
* Frequent reaching, high, low, and level.
* Frequent audio acuity at all ranges, including speech.
* Frequent visual acuity for reading.
* Constant sitting.
* Constant use of clear oral communication.

## TOOLS AND EQUIPMENT USED

* Standard office equipment.
* Small hand tools.