EL CAMINO COLLEGE

JOB TITLE: INFORMATION SECURITY OFFICER

Classification:	Classified Administrator	Retirement Type:	PERS*
Salary Range:	11	Board Approved:	January 18, 2022

BASIC FUNCTION:

Under the direction of a designated administrator, the Information Security Officer develops and implements procedures, policies, strategies, and standards in the management of the College's IT security program and controls. Assesses and recommends strategies to address IT-related risks, threats, and other identified operational deficiencies; develops, coordinates, and leads incident response activities; develops campus-wide IT security plans; monitors systems and ensures compliance with relevant regulatory requirements and standards; and fosters an IT compliance-focused campus culture through end-user education programs. Supervises assigned staff and/or teams.

REPRESENTATIVE DUTIES:

Collaborates with the College's academic and administrative units and relevant ITS support teams to facilitate IT risk assessments. Implements risk management processes and best practices. Identifies location, type, sensitivity, ownership, and access requirements for data being used by the College. Establishes controls and standards in consultation with supervisor, division/department personnel, and other key constituencies as appropriate.

Monitors the external IT environment for emerging threats. Effectively configures and utilizes available systems, alerts, and other sources of information to identify and address security threats and events. Advises supervisor on appropriate course of action. Documents risk analysis of security threats for management review.

Researches, evaluates, and recommends appropriate IT security systems, technology, controls, and solutions (e.g., firewalls, intrusion detection/prevention, and vulnerability scanners.) Provides detailed pros and cons, build vs. buy analyses of options. Ensures plans and designs consider security controls, performance, confidentiality, scalability, access, cost, etc.

Oversees the implementation of security testing projects and other system plans. Validates project adherence to District policies and standards. Ensures regulatory compliance through thorough testing, assessment, and remediation prior to full implementation.

Develops, implements, and manages College-wide IT security incident response processes and procedures. Leads the investigation, coordination, resolution, and closure on security incidents as they are escalated or identified. Generates fact-based reports. Documents incident response processes/protocols and updates as needed.

Develops, implements, and maintains a College-wide IT security plan and obtains plan sign-off from key stakeholders and constituencies, as appropriate. Executes a plan that ensures the

integrity and confidentiality of information residing in College workstations, servers, mobile devices, and related computer peripherals.

Maintains an in-depth technical documentation repository of College systems, networks, and core applications.

Leads the planning, testing, and tracking of periodic, College-wide IT security audits. Identifies security gaps and deficiencies through risk assessments and recommends corrective action of identified vulnerabilities and weaknesses. Ensures requisite compliance monitoring is in place to expeditiously identify control weaknesses, compliance breaches, misuse trends, and/or operational loss events.

Serves as a subject matter expert on District strategies for information security processes. Ensures implemented processes align to regulatory Federal, State, and industry requirements and District policies.

Leads the review and formal approval process for policy and procedural updates to meet or exceed industry standards, compliance requirements, and end-user expectations.

Develops, implements, and manages a College-wide IT security awareness and training program that fosters a risk and compliance-focused culture. Ensures training programs align information security activities with regulatory requirements and internal risk management policies. Provides regular guidance, resources, and advocacy on current best practices for information security.

Assists with the development and implementation of business continuity and disaster recovery plans to ensure comprehensive information security and mitigation of risks. Assesses and manages the adequacy of mitigation and remediation plans of known cyber security vulnerabilities and threats.

Serves as a contributing member of the ITS management team in the development, prioritizing, budgeting, and planning of IT security strategies and related initiatives.

Ensures information security risks, recommendations, and mitigation technologies are identified, articulated, and communicated through the District's governance process. Develops and communicates current IT security posture status, IT security strategies, and progress on IT security initiatives to key organizational units, executive management, and the College Board of Trustees, as needed.

Establishes and maintains appropriate network of professional contacts. Collaborates with other colleges and universities to share information or resources, as appropriate. Develops and manages partnerships with IT security vendors and consultants.

Maintains awareness and knowledge of current changes and best practices within legal, regulatory, and technology environments which may affect the security of IT systems, networks, and overall operations. Ensures supervisor and staff are informed of any changes and updates in a timely manner. Attends conferences and trainings as required to maintain IT security management proficiency.

Serves on IT security-related college committees as appropriate.

Performs other related duties as assigned or requested.

JOB QUALIFICATIONS:

Education and Experience:
Bachelor's degree in an IT related field.
Five (5) years of experience in IT networks, systems, or security-related positions.

OTHER QUALIFICATIONS:

Licenses or Other Certifications:
CISSP (Certified Information System Security Professional) desirable, but not required.
CISM (Certified Information Security Manager issued by ISACA) desirable, but not required.
CISA (Certified Information Security Auditor issued by ISACA) desirable, but not required.
Valid California driver's license.

Knowledge/Areas of Expertise:
Knowledge of IT environment in higher education or other public/government agency.
Knowledge of information security, governance, risk and compliance practices and standards.
Knowledge of relevant laws/regulations (e.g., FERPA, HIPAA, GLB Act, Sarbanes-Oxley.)
Knowledge of IT risk and control frameworks (e.g., CoBIT, ISO, NIST, ITIL, PCI.)
Knowledge of information security regulatory requirements and standards.
Knowledge of effective IT security systems, network architectures, concepts, techniques, tools.
Knowledge of IT security management industry best practices and standards.
Experience with development of educational programs in the area of security awareness.
Experience with institution-wide networks, systems, and applications.
Experienced in developing and implementing IT security policies and procedures.
Experienced in IT security auditing and monitoring.
Experienced in managing network and system security components (e.g., firewalls, intrusion detection/prevention systems.)

Abilities/Skills:
Ability to identify, prioritize, and communicate impact of IT security risks and exposures.
Ability to maintain compliance with applicable IT security-related laws and regulations.
Skilled at organizing and communicating status on IT security strategies and projects.
Skilled at developing and testing business continuity and disaster recovery plans.
Skilled at analyzing, planning, and organizing.

WORKING CONDITIONS:

May be required to drive to offsite locations; must have reliable transportation.
Extensive computer work.
Use of hands, wrists, and fingers to operate various machines and equipment.
Extensive interaction with a variety of individuals.
Movement from one work area to another.

* Previous employment performed in a different public retirement system may allow eligibility to continue in the same retirement system.