Contra Costa Community College District
Classification Specification

Information Security Officer

Class Code	OT Status	EEO Category	Represented Status	Salary Grade	Effective Date	Status	Pages
	Exempt	Officials & Administrators	Management	M7	**08/30/07**	Management	1 of 1

DEFINITION: Under direction, administers and oversees the District's information security program in a multi-college environment. The incumbent is responsible for developing information security policies and guidelines, growing the District-wide information security program, further developing the security architecture and advancing information security education for the District.

PURPOSE: Incumbents in this classification develop and implement a District-wide security program that supports the academic and administrative use of information technologies in a distributed client/server environment. Working in conjunction with technology staff and personnel at each site, the incumbent assumes overall responsibility for ensuring processes are in place to assess and monitor the security of the District's computers, networks, and data; formulates and disseminates District standards for security, and reviews relevant policies and procedures in the context of these standards; educates, advises and trains staff on approaches for ensuring the security of District networks, systems, and data; develops crisis management procedures; assists with emergency response and disaster recovery; directly assists in resolution of serious incidents; leads projects concerning the evaluation and implementation of security-related technologies.

EXAMPLES OF DUTIES/ESSENTIAL FUNCTIONS: Duties/essential functions may include, but not be limited to, the following:

- Working with all District sites, formulate and disseminate District-wide standards for security and access control, and review relevant policies and procedures in the context of these standards;
- Provide leadership and participate effectively with Information Technology staff in network design and engineering to insure appropriate levels of security are in place and maintained;
- Assess the security of district-wide computers, networks, and data as well as personal workstations that access and/or store data. Define and advocate "best practices" regarding security of data and systems. Promote security awareness;
- Participate in assessment and acquisition of information security hardware and software. Assist in setting priorities for use of resources. Ensure the implementation of features and products provide appropriate controls over systems and networks;
- Develop and document strategies to mitigate network attacks and breeches including but not limited to denial of service, network intrusion, worm attack, network spoofing, spam/phishing;
- Implement security and network management systems to track and monitor network disruptions and identify network anomalies which should generate alerts and response;
- Perform risk analysis of new technologies;
- Develop procedures to handle crisis situations. Organize task forces and coordinate investigations with District Police, Human Resources, and/or Internal Auditor;
- Advise senior executives on security issues and/or events. Keep District Police informed of technical developments in computer/network security;
- Coordinate the development and testing of information systems business continuity policies, plans, and procedures;
- On a continued basis, be cognizant of all state and federal laws and mandates regarding privacy and the protection of critical personal data;
- Monitor and report on College and District information security activities and compliance;
- Aggressively apply available technologies, processes and procedures to protect all district-wide data, information and image storage;
- Perform other duties as assigned.

Information Security Officer

Class Code	OT Status	EEO Category	Represented Status	Salary Grade	Effective Date	Status	Pages
	Exempt	Officials & Administrators	Management	M7	08/30/07	Management	2 of 2

MINIMUM QUALIFICATIONS:

Knowledge Of: Computer information security, including experience with internet technology and security issues. Experience with security planning and development of policies, as well as experience managing large scale projects.

Ability To: Plan and develop policies and procedures; analyze situations accurately and make independent decisions; establish and maintain effective working relationships with those contacted in the performance of required duties; communicate effectively verbally and in writing; coordinate collaborative initiatives to advance information security strategies for a large, decentralized organization; understand and implement cultural change related to technology with an awareness that developing strong security practices involves both technology and people.

Education/Training/Experience: BA or BS in Computer Science, Computer Information Systems, or related field. Experience managing large scale projects. Five years of progressively responsible relevant experience in an information systems security environment offering technical and analytical support and leadership.

Desired Qualifications: *Preference will be given to candidates who have a CISSP, CISA, CISM or other security certifications. Experience with business continuity planning, auditing and risk management.*