**Position Description**

Report Run Date: Mar 1 2016 5:02PM

Position Number: 02019002

Dept: ENT APPS & INFRASTRUCTURE SVCS - 061419

Position: ASSISTANT CHIEF INFORMATION SECURITY OFFICER

Approved Payroll Title Code: 6019

Approved Payroll Title: IT SECURITY MGR 1

Approved MSP Salary Grade: MSP26

**POSITION DETAILS**

Under the general direction of the Chief Information Security Officer (CISO), this leadership position develops and implements security and data protection solutions that support the mission of the university and protect the confidentiality, integrity, and availability of information assets owned or entrusted to UC Davis. The Assistant Chief Information Security Officer works with campus stakeholders to ensure data security needs and controls are aligned to support organizational goals and objectives and provides input to campus-wide and departmental strategic plans, audits, and reviews. Also leads the planning and execution of projects and operational services in the areas of information security operations, risk management, compliance management, and incident management.

Job Summary:

Campus Job Scope:

This position provides leadership, vision, and guidance on information security matters. The Deputy/Assistant Chief Information Security Officer develops new services, standards, and operating procedures that enable the campus to effectively and efficiently address information security risks and comply with laws and regulations governing data protection.

Department Specific Job Scope:

This position must work collaboratively across department and division boundaries with campus stakeholders and leaders to identify and build on opportunities that strengthen the campus security posture and ensure campus information assets are protected from unauthorized access, modification,
or disclosure. The Deputy/Assistant Chief Information Security Officer provides guidance and assess client requirements to determine if additional security services are needed and to promote use of good security practices where required.

The Deputy/Assistant Chief Information Security Officer must be a leader and create a positive environment where members of the security team can enhance their skills as future leaders.

The Deputy/Assistant Chief Information Security Officer operates with a high degree of autonomy, uses independent thinking to creatively solve problems and issues, makes independent decisions, and must maintain or preserve confidentiality when required to do so.

The Deputy/Assistant Chief Information Security Officer must stay abreast of evolving campus needs, technology capabilities, and threat intelligence from a variety of sources to optimize data protection measures. Collaborate with management teams and technical leads from campus academic and administrative divisions on data protection measures. Provide direct management of the newly formed Information Security Professional Services team and indirect management of the Information Security Operations unit in support of a wide range of projects and initiatives designed to protect the confidentiality, integrity, and availability of campus information assets.

Positions Supervised: TBD

Essential Responsibilities:

50% LEADERSHIP
Mgmt of Security (IS) Professional Services team & indirect mgmt of IS Operations unit in support of a wide range of projects & initiatives designed to protect confidentiality, integrity & availability of campus information assets
Develop policies, procedures, direction & scope of work, adapt unit's goals, priorities & scope of work to meet larger, UCD objectives
Supervise staff & ops of the IS group. Delegate work & set priorities.
Provide guidance to employees in conduct of their jobs & development of their skills; address & resolve problems; assure accountability; provide corrective action
Support/implement affirmative action goals in selection & promotional ops
Partner on data protection measures & joint projects across campus & UCDHS
Work with legal, audit, etc to align the IS program with campus goals
Point of escalation for client issues & resolve disputes /service issues that arise
Facilitate campus-wide service collaboration & communication
Recommend policies, standards & procedures governing the protection of campus information assets in accord with security, ITIL & industry standards
Develop resource plans, project plans & budgets; present proposals, prepare documents & obtain campus & mgmt consensus
Represent campus at all meetings /conferences

30% RISK, COMPLIANCE & INCIDENT MGMT
Support the development of an IT & security risk assessment framework & assess regulatory & organizational IT & security risks, conduct security assessments & implement solutions to assist with the improvement of the security infrastructure
Manages & supports activities designed to enhance the security posture thru input to departmental & campus-wide strategic plans, audits & reviews; preparing & completing action plans; resolving problems; identifying trends; determining system improvements; & implementing change
Develop, monitor & assess campus processes governing IS risk assurance. Assess threats & risks; identify vulnerabilities; perform risk assessments; perform vendor based risk assessments; perform campus based compliance assessments against laws, regulations, & industry frameworks
Develop & direct the campus IS control monitoring programs to ensure compliances are being met & identified risks managed
Oversee selection & ops of tools to facilitate sec monitoring
Identify security compliance control gaps & oversee the documentation, implementation & testing of the UCD security compliance control & risk portfolio
Identifies where existing policies & procedures require chg to reduce security threats & keep the campus compliant with applicable laws & regulations. Develop & implement eDiscovery response plans
Evaluate & use e-discovery technology tools, incl identification & collection, searching & culling early case assessment, processing & production tools

10% SECURITY ADMIN
The IS Operations team performs mgmt of some central systems, for over 50,000 users, including a cluster of systems that test for vulnerabilities. Major functions:
Establish tech direction & strategies for the ops team; provide strategic direction for adoption & integration of new security technologies; provide support for planning & development of enterprise IS services; mentor/guide specifications & early design of projects for security technologies
Supervise detection & correction of security incidents on UCD systems, firewalls & networks, forensic analysis, firewall policy & security configuration & the implementation & mgmt of campus security services such as the Intrusion Prevention System, Honeypot & the campus network scanners
Recommend solutions for tech problems & implement solutions
Throughout service life-cycle, understand dependencies of tech objectives to make decisions
10% OTHER DUTIES
Supports the UCD & IET's Mission & Values & the Principles of Community. Maintain currency in tech skill areas.

Physical Demands:
- Work alternate or extended hours on short notice.
- Occasional travel is required to campus and off campus worksites.
- Due to the mission-critical services provided by this department, this position may work hours other than M-F 8-5, especially during system development, hardware or software installation, or in response to system problems.

Work Environment:
UC Davis is a smoke and tobacco free campus effective January 1, 2014. Smoking, the use of smokeless tobacco products, and the use of unregulated nicotine products (e-cigarettes) will be strictly prohibited on any UC Davis owned or leased property, indoors and outdoors, including parking lots and residential space.

Background Check: Yes

QUALIFICATIONS
Minimum Qualifications:
- Experience of applicable business processes and operations of customer organizations
- Experience of information security program management and project management principles and techniques
-Experience using industry-standard and organizationally accepted analysis principles and methods
-Strong business management and leadership experience in a self-supporting operation;
-Experience in supervision/leadership and human resource management of highly technical staff to hire, assign and direct work, evaluate and reward performance, transfer or promote, suspend, layoff/recall, discharge, or otherwise discipline career staff employees.
-Experience to meet customer/client expectations with an emphasis on quality, quantity and timeliness of work.
-Experience managing workgroup initiatives and projects
-Interpersonal and written communication skills to communicate complex technical information to all hierarchical and technical levels at the organization and to prepare and present written and oral reports
-Knowledge of Information Assurance principles used to manage risks related to the use, processing, storage, and transmission of information or
-Knowledge of different classes of cyber attacks (e.g., passive, active, insider, close-in, distribution)
-CISSP, CISM, CISA or GIAC certifications
-Bachelor's degree in related area and/or equivalent experience/training.
-Skill to work effectively with broad-based constituencies and the highest levels of executive management.
-Skill to present information effectively and tailor presentations to a wide variety of audiences (including executive management).

Expected Qualifications for Selection:

Expectations

Job Expectations

-Read and follow the UCD Principles of Community
-Diplomatic oral and written communication skills for interactions with others.
-Accountability for the safekeeping of resources in the employee's care and custody and for following and implementing the cyber-safety guidelines.
-Excellent organizational and analytical skills.
-Communicate with users in non-technical terms on technical issues.
-Communicate on a technical level with other knowledgeable persons.
-Excellent skills to establish priorities, organize tasks, and
direct effective implementation of tasks in a demanding work environment.
- Willingness to learn and apply new technology and willingness to develop skills to promote professional growth.
- Willingness to routinely stay in communication with technical staff at other organizations to stay abreast of computing developments and resources available over the network.
- Excellent communication (oral, written, presentation, documentation) and interpersonal skills, using tact and diplomacy for interactions with clients and vendors.
- Independently follow projects through to successful completion with a high degree of quality.
- Experience learning from technical manuals, journals and continuing education and apply that information.
- Work in a team environment to provide complex distributed and integrated mission-critical services and to solve technical problems in this environment.
- Maintain flexibility in a continuously changing and fast paced work environment.
- Make well planned decisions.
- Work with a diverse group of people in such a manner as to build high morale and group commitments to goals and objectives.
- Work cooperatively with others to achieve and maintain a strong client service environment.