Position Description

Position Description	
Requisition Number:	03024723
Position Number:	02024377
Dept:	ENT APPS & INFRASTRUCTURE SVCS - 061419
Position:	SENIOR INFORMATION SECURITY CONSULTANT
Approved Payroll Title Code:	0662
Approved Payroll Title:	IT SECURITY ANL 5
Approved MSP Salary Grade:	
Approved PSS Salary Grade:	MSP27
POSITION DETAILS	
Job Summary:	The Senior Information Security Consultant (Senior ISO) is a visionary and experienced in delivering high-performing cybersecurity services designed to support the mission of the university and protect the confidentiality, integrity, and availability of information assets created or managed by faculty, staff, students, and business partners. The Senior ISO works on complex cyber challenges facing UCD and leads (or support) critical information security services of significant importance to UCD. This individual helps develop the University's global information security strategy and works as part of a team to actively identify and mitigate geopolitical cyber threats UCD's information assets. The Senior ISO provides guidance and assess client requirements to determine if additional security services are needed and promotes good security practices where required. The Senior ISO interacts with all levels of the University, peers at other UC campuses, and UCD business partners to establish and maintain a strong and adaptive security posture that aligns with organizational risk tolerance, information access requirements, and business/academic strategies. The Senior ISO supports UCD researchers across the globe by advising on cyber related matters. This individual is responsible for evaluating research environments and support researchers in meeting compliance requirements. The individual in this role also supports the development and execution of an information security strategy for the Aggie Square Information Security Program, and assumes responsibility for the ongoing development and implementation of the Aggie Square information security service portfolio. As a member of the UCD Information Security team, the Senior ISO develops new services and operating procedures that address information security risks and comply with laws and regulations governing data protection. The Senior ISO will serve as subject matter expert and trusted advisor to university officials (including the UCD Health System) on security-related matters, and maintain relationships with local, state and federal law enforcement and other related government agencies by actively representing UC Davis within the industry. This individual debriefs the Chief Information Officer (CIO)/Cyber Risk Responsible Executive (CRE) and Chief Information Security Officer (CISO) on current and emerging information security matters, provides reports to management regarding the effectiveness of the information security program, and makes recommendations for the adoption of new procedures and technologies as required. As a member of the Information Security leadership team, the Senior ISO participates in strategic planning, leads teams, develops/manages budgets, and manages a security solutions portfolio. The Senior ISO must stay abreast of geopolitical cyber issues, UC policies and initiatives, evolving campus needs, technology capabilities, and threat intelligence from a variety of sources, to optimize data protection measures. This individual will use independent thinking to creatively solve problems and issues, make

	independent decisions, and must maintain or preserve confidentiality when required.
Campus Job Scope:	
Department Specific Job Scope:	
Positions Supervised:	N/A
Essential Responsibilities:	50% STRATEGIC PLANNING, LEADERSHIP & MANAGEMENT Develop and manage an information security vision and strategy that aligns with the university's priorities and objectives for conducting research securely and meets international, federal, and state compliance obligations. Disseminate cyber-intelligence, and promote information security services, by communicating regularly with all stakeholders. Advise executive management of changes in threat intelligence and in the technical, legal, and regulatory landscape. Interact with campus researchers, Aggie Square occupants, and university officials to ensure the development and consistent use of information security services. Collaborate with Aggie Square occupants and campus officials to effectively balance the business needs of Aggie Square's occupants with UC/UC Davis policies, with a focus on adherence to regulatory and compliance needs. Identify and advocate for investments in security tools and services to meet the growing needs of UCD's research community and achieve the Aggie Square security strategy. Promote global awareness of information security. Define information security metrics, and periodically update senior leaders (e.g., Vice Chancellors), the UC Davis Cyber Risk Responsible Executive, and Aggie Square Board of Directors on the security strategy. Create and manage a targeted information-security awareness program for faculty, staff, students, and Aggie Square occupants and establish metrics to measure the effectiveness of this security training program. Engage third-party security vendors in assessing solutions against current or future needs Actively conduct risk assessments on research projects and security services designed for the Aggie Square campus. Identify, prioritize, and mitigate cyber-risks with stakeholders, and instill a risk-aware culture. Collaborate with the information risk management and compliance groups to identify, prioritize, and respond to risk components, and to develop security architecture and process in support of business strategy. Serve as a subject matter experts to research teams and participate in the Aggie Square campus Architectural Review process to ensure that facility, network, and communication plans incorporate information security controls. 45% INCIDENT RESPONSE & CYBER THREAT MANAGEMENT Investigate, support, and consult with senior management during cyber-incidents. Oversee the monitoring of university-wide security tools and investigate breaches of security controls, taking action according to university-established process and procedure. Monitor the cyber-threat environment for emerging threats and advise relevant stakeholders on the appropriate courses of action.

	Oversee assessment of cyber-threats to the organization, including near-term and strategic risks within critical functions. Develop and maintain broad strategic and tactical plans; internal processes; and staff capabilities to support security advisories (vulnerability intelligence), cyber-threat analyses, security recommendations, cyber-intelligence briefings, and information sharing with trusted partners. Provide support managing or directing response activities during cyber-incidents or emerging cyber-threat conditions. Deliver high-impact written and verbal briefings on sensitive cyber-threat intelligence matters with a broad range of audiences, including information security staff, senior executive leadership (e.g. CIO, CISO) and business area representatives. 5% OTHER DUTIES Supports the UCD & IET's Mission & Values & the Principles of Community. Maintain currency in tech skill areas. Other duties and special projects as assigned.
Physical Demands:	
Work Environment:	This position is a critical position and subject to a background check. Employment is contingent upon successful completion of background investigation including criminal history and identity check. 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. 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:	Bachelor's degree in related area or an equivalent experience and education. Knowledge/understanding of relevant legal/regulatory requirements (e.g., FERPA, HIPAA, PCI, and FISMA). Knowledge of common information security frameworks, such as ISO/IEC 27001, ITIL, and NIST. Expert knowledge and demonstrated experience selecting and applying appropriate security controls and demonstrated skill in developing security policies and procedures. Demonstrated skill at analyzing and preventing security incidents of high complexity. Advanced experience in incident response and digital forensics including reporting. Experience presenting to and advising leadership on complex information.

	Experience working effectively with both technical and non-technical personnel at various levels in the organization. Experience leading cross-functional interdisciplinary teams Experience working with service providers. Excellent written/verbal communication skills, interpersonal/collaborative skills, and ability to communicate security/risk-related concepts to technical and nontechnical audiences. Experience working with or at a university or medical center. Experience handling confidential matters
Preferred Qualifications for Selection:	Minimum of one professional certification (e.g., CISSP, CISM, CISA, ISA, or similar credentials). Possess a security clearance. Experience in finance/budget/resource management. Experience meeting client expectations, with an emphasis on quality and timeliness of work.

Expectations

Job Expectations	- Read and follow the UC Davis Principles of Community - 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.