Chief Information Security Officer

Job Category: Managerial/Professional
Unit: Information Technology
Position Code: SIT0013
Status: Open
Closing Date: 12/2/2018
Salary: $120,000 + (Commensurate with Education and Experience)
Location: Merced

Background check: Background check and fingerprinting may be required

Description: The Chief Information Security Officer (CISO) provides guidance and counsel to the Chief Information Officer (CIO) and key members of the university leadership team. The CISO reports directly to the CIO and leads the information security planning processes to establish an inclusive and comprehensive information security program in alignment with University of California System-wide Information Security Policy IS-3. The CISO establishes campus policies and procedures to maintain the confidentiality, integrity and availability of university data across academic, research, and administrative information systems and technology. The CISO has functional responsibility for the management and delivery of information security outcomes executed by direct reports as well as indirect efforts carried out by other OIT staff and campus units.

KEY RESPONSIBILITIES

- Directs the mitigation efforts that may compromise security protocols. - Leads the development, implementation, and evaluation of campus-wide Risk Management Processes.

- Promotes collaborative, empowered working environments across campus removing barriers and realizing possibilities.

- Ensures appropriate staffing sufficient for compliance with cyber security standards and procedures.

- Directs UC Merced's Campus Identity and Access Management program.

Qualifications:
- Bachelor's degree in Computer Science related discipline (Master's preferred).

- 10 years of experience working in a complex IT organization with at least 5 years of Cyber Security Leadership.

- Demonstrated knowledge of IT Security controls and practices.

- Advanced interpersonal skills sufficient to work effectively with both technical and non-technical personnel at various levels in the organization.

- Expert knowledge of IT security systems and tools including firewalls, intrusion prevention systems, SIEM, and vulnerability management platforms.

- Demonstrated skills directing and applying security controls to Computer software and hardware utilizing the NIST Cybersecurity framework or ISO 27001.

- Demonstrated skill at administering complex security controls and configurations to computer hardware, software and networks.

- Advanced knowledge of data encryption technologies and experience selecting and applying appropriate data encryption technologies to endpoints, databases, transport protocols, etc.

- Advanced experience directing incident response and digital forensics.

- Demonstrated knowledge of secure hardware, software and network design techniques.

- Demonstrated strategy for analyzing and preventing security incidents in highly complex environments.

- In-depth knowledge of computer hardware, software and network security issues and approaches.

- Experience interfacing with upper management on a regular basis. Broad knowledge of other areas of IT.

- Advanced experience assessing institutional risk and recommending appropriate remediation or compensating controls.

PREFERRED QUALIFICATIONS

- Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or similar.

- Knowledge of UC IS - 3 Policy, processes and procedures, or corresponding policy of import.

To Apply: Please complete a UC Merced application and email along with resume and cover letter to ucmcareers@ucmerced.edu. Please indicate in the subject line of your email the Position Title and Position Number you are applying for. For questions regarding how to apply please email ucmcareers@ucmerced.edu or call 209-228-8247.

If you do not have internet access you may mail your application, resume, and cover letter to: University of California, Merced, 5200 North Lake Rd., Merced CA 95343. Please list the job number on the subject line.

As of January 1, 2014 the University of California, Merced will be a smoke and tobacco free workplace. Information and the Smoke and Tobacco Free policy is available at http://smokefree.ucmerced.edu

E-Verify: Effective September 8, 2009, all employers who receive Federal contracts and grants are required to comply with E-Verify, an Internet-based system operated by the Department of Homeland Security (DHS) in partnership with the Social Security Administration (SSA). E-Verify electronically verifies employment eligibility by comparing information provided on the I-9 form to records in the DHS and SSA databases. Certain positions funded by federal contracts/subcontracts requires UC Merced to notify job applicants that an E-Verify check will be conducted and the successful candidate must pass the E-Verify check. More Information

For information on the comprehensive benefits package offered by the University of California visit:
http://atyourservice.ucop.edu/forms_pubs/misc/benefits_of_belonging.pdf