UNIVERSITY OF SOUTHERN CALIFORNIA

Data Protection Manager

Job Code: 166040

OT Eligible: **No**

Comp Approval: **10/26/2020**

JOB SUMMARY:

Oversees the implementation of safeguards to secure high-value university assets. Manages data discovery, analysis and mapping of across the university and onboarding into the high-value asset program. Maintains strong partnerships with the broader university data privacy program. Provides leadership and oversight of local school/unit data protection requirements.

JOB ACCOUNTABILITIES:

*E/M/NA	% TIME	
_____	_____	Defines, operates and implements comprehensive data protection strategies and programs to prioritize and mitigate cyber risk relevant to high-value and confidential information (e.g., student data, protected health information, critical research data). Creates and maintains high-value asset program, controlling assessment in line with the university's risk framework. Serves as a subject matter expert (SME) on data protection strategies to ensure process alignment with regulatory, statutory, and industry requirements and university policy and data classification.
_____	_____	Partners with other departments for risk assessment and remediation plans to reduce risk related to high-value data/assets. Tracks and maintains milestones, metrics, key performance indicators (KPIs), and associated budget and resource impacts to maintain effective data protection program. Partners with risk management and compliance advisory, key stakeholders and partner function teams to manage relationships and share information. Oversees third-party resources assisting the implementation of data protection program initiatives.
_____	_____	Advises on matters relating to the investigation, impact, and analysis of decisions regarding high-value data protection. Manages the asset scorecard reporting program to ensure the implications of safeguards implementation are understood, risks are reported to and managed at the correct level within the organization, and risk acceptances for high-value assets are tracked and reported on throughout their lifecycle.
_____	_____	Defines and manages application security standards and requirements and data-loss prevention enterprise program requirements. Oversees enterprise-level components to integrate operational components of application security and data loss prevention testing, tuning, and monitoring, in collaboration with security operations team.
_____	_____	Maintains currency with changes in legal, regulatory, and technology environments which may affect operations. Ensures senior management and staff are informed of any changes and updates in a timely manner. Establishes and maintains appropriate network of professional contacts. Maintains membership in appropriate professional organizations and publications. Attends meetings, seminars and conferences and maintains continuity of any required or desirable certifications, if applicable.
_____	_____	Promotes an environment that fosters inclusive relationships and creates unbiased opportunities for contributions through ideas, words, and actions that uphold principles of the USC Code of Ethics.

Performs other related duties as assigned or requested. The university reserves the right to add or change duties at any time.

***Select E (ESSENTIAL), M (MARGINAL) or NA (NON-APPLICABLE) to denote importance of each job function to position.**

EMERGENCY RESPONSE/RECOVERY:

Essential: ☐ No

☐ Yes In the event of an emergency, the employee holding this position is required to "report to duty" in accordance with the university's Emergency Operations Plan and/or the employee's department's emergency response and/or recovery plans. Familiarity with those plans and regular training to implement those plans is required. During or immediately following an emergency, the employee will be notified to assist in the emergency response efforts, and mobilize other staff members if needed.

JOB QUALIFICATIONS:

Minimum Education:

Bachelor's degree

Combined experience/education as substitute for minimum education

Minimum Experience:

5 years

Minimum Field of Expertise:

Five years' experience in a data protection environment, performing information security controls evaluation. Extensive analysis and assessment experience. Experience with problem identification and resolution. Leadership and project management experience. Excellent written and oral communication skills.

Preferred Education:

Bachelor's degree

Preferred Experience:

7 years

Preferred Field of Expertise:

Advanced knowledge of information security, data protection, data privacy, risk management. Large enterprise or complex entity related experience. Experience in higher education.

Supervises: Level:

Manages through subordinate supervisors.

SIGNATURES:

Employee: _____ **Date:** _____

Supervisor: _____ **Date:** _____

The above statements are intended to describe the general nature and level of work being performed. They are not intended to be construed as an exhaustive list of all responsibilities, duties and skills required of personnel so classified.

The University of Southern California is an Equal Opportunity Employer