



JOB INFORMATION

Job Code:	166041
Job Title:	Data Protection Lead
FLSA Status:	Exempt
Supervisory:	May oversee student and/or temporary workers.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

The Data Protection Officer is responsible for defining and implementing data protection policies and standards across various technologies and systems within the university. Responsibilities include maintaining high-value asset (HVA) programs, designing data protection solutions to manage data transmission and disposal, managing the implementation of data protection technologies and processes, and overseeing risk mitigation efforts. This position is also responsible for staying abreast of applicable privacy regulations, serving as the SME and establishing coordinated efforts to educate and campaign for risk awareness across the university's departments, schools, and units. The Data Protection Officer is accountable for managing third-party relationships, including reviewing and validating NDA agreements.

JOB QUALIFICATIONS:

Education

Req	Pref	Degree	Field of Study
X		Bachelor's degree	
	X	Bachelor's degree	

Additional Education

Check here if experience may substitute for some of the above education.

Combined experience/education as substitute for minimum education

Work Experience

Req	Pref	Work Experience	Experience Level
X		5 years	
	X	10 years	

Additional Work Experience

Check here if education may substitute for some of the above work experience.

Combined experience/education as substitute for minimum work experience

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Knowledge of compliance frameworks and security management standards (e.g., ISO 27001:2013, COBIT, NIST).
X		Strong experience and knowledge of Configuration Management methodologies and implementation.

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Demonstrable knowledge of laws relating to privacy, intellectual property protection and cybercrime.
X		A solid technical foundation in data loss prevention, including hands-on experience with at least one Enterprise DLP solution, management of an information protection program and supporting information protection processes, or commensurate experience in DLP/information protection support for an organization.
X		Possesses knowledge in key data protection concepts, such as high-risk data and communication handling requirements, data classification strategy, data handling and labelling and encryption mechanisms, e.g., cryptography and key management.
X		Understanding of security technologies for protecting data at rest, transit and in use.
X		Experience working with and/or implementing DLP tools and solutions within On-Prem or Cloud Based solutions such as O365 and G Suite.
X		Demonstrable understanding of Cryptography related to a data protection program.
	X	Advanced report writing experience.
	X	Experience in using and Microsoft Dynamics CRMStrong.
	X	Information Security Industry background including one or more Security certifications (CISSP, CISM, CISA).
	X	Solid understanding of Security concepts.
	X	Awareness and knowledge of ServiceNow GRC.
	X	Demonstrable understanding of networking and large scale systems.

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Determines, defines and implements data protection strategy and approve data protection policies and standards across various technologies, including but not limited to; O365, G Suite, On-Prem, Legacy Systems, etc.; routinely reviews data protection strategy for the enterprise.				
Maintains high-value asset (HVA) data program, advising, developing and overseeing plans to mitigate risks within the HVA data assets.				
Designs Enterprise data protection technology solutions to protect the collection or creation, storage, use, transmission and disposal of data.				
Organizes and oversees the management and implementation of Enterprise DLP technologies and processes. Tests and reviews DLP rules, and provides oversight to the managed services provider.				
Coordinates with Schools, Services, and Administration teams to manage relationships and share information. Serves as a subject-matter expert pertaining to the program's objectives and associated control requirements of which the Schools, Services, and Administration functions are held responsible. Proactively reviews internal processes and activities to identify opportunities for improvement.				
Keeps up-to-date with data protection and privacy regulations, laws, standards, and industry trends. Influences behavior to reduce risk and foster a risk management awareness throughout the organization.				
Provides ongoing education and awareness on Data Protection Program control objectives and expectations through awareness campaigns across departments, schools, and units.				
Provides expert advice and support in the review of suspected and escalated alerts, events and incidents.				
Reviews contracts and non-disclosure agreements (NDAs) with third parties to validate appropriate data protection clauses and audit rights are included in coordination with third party management within Information Security Governance and Risk Management (ISGRM) team. Works closely with Service Management and other teams to continually enhance and expand upon the CI methodology and implementation as it relates to the use by a DLP solution and data protection program.				
Conducts independent reviews of HVAs to validate compliance with security policies and procedures in conjunction with security based risk assessments driven by the ISGRM team.				

JOB ACCOUNTABILITIES

	<i>% Time</i>	<i>Essential</i>	<i>Marginal</i>	<i>N/A</i>
Maintains awareness and knowledge of current changes within 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.				

Other Requirements

<i>Essential:</i>	<i>Emergency Response/Recovery</i>	<i>Essential:</i>	<i>Mandated Reporter</i>
	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.		A mandated reporter who in his or her professional capacity has knowledge of, or reasonably suspects a person who is under the age of 18 years, elderly, or a dependent adult has been the victim of abuse or neglect must report the suspected incident. The reporter must contact a designated agency immediately or as soon as practically possible by telephone or in writing within 36 hours. By virtue of the associated job duties, this position qualifies as a mandated reporter as required by state law and USC's policy at: https://policy.usc.edu/mandated-reporters/
<i>Campus Security Authority (CSA)</i>			<i>Essential:</i>
By virtue of the associated job duties, this position qualifies as a Campus Security Authority as required by law and USC's policy at: https://dps.usc.edu/alerts/clery/			No

ACKNOWLEDGMENTS

The above statements reflect the essential and non-essential functions as necessary to describe the principle contents of the job. They are not intended to be a complete statement of all work requirements or duties that may be required of the position. I understand that I may be asked to perform other duties as assigned. USC reserves the right to add or change duties at any time.

The University of Southern California is an Equal Opportunity Employer. USC prohibits discrimination on any basis protected under federal, state, or local law, regulation, or ordinance or university policies. All employment decisions are based on individual qualifications and business need.

I acknowledge receipt of this job description and its associated physical requirements. I have read and understand the job description and job requirements and agree to abide by their contents. I realize that duties may be requested of me that are not specifically stated herein. I understand that I will be expected to adjust to potential fluctuations in work volume. I understand that, if I have any questions about the essential functions or expectations of my position, my supervisor and/or HR partner are available to discuss them with me.

Print Employee Name

Signature

Date

Print Manager Name

Signature

Date

This job description describes the general nature and level of work required by the position. It is not intended to be an all-inclusive list of qualifications, skills, duties, responsibilities or working conditions of the job. The job description is subject to change with or without notice, and Management reserves the right to add, modify or remove any qualification or duty. Nothing in this job description changes the existing at-will employment relationship between the university and the employee occupying the position.