HEALTH CENTER PARTNERS of Southern California

A Family of Companies

HCP IHP HQP

JOB DESCRIPTION

JOB TITLE:	Information Security Analyst		**COMPANY:**	HCP
REPORTS TO:	HCP AVP for Enterprise Operations			
DIRECT REPORTS:	None			
STATUS:	Non-Exempt	FULL TIME	**WORK COMP CLASS:**	8810
OUTSIDE TRAVEL:	0%	**SCHEDULE :** 7-7/M-F	**WORK CONDITIONS:**	Remote/Home Office
This job description is intended to be a general statement about this job and is not to be considered a detailed assignment. It may be modified at any time, with or without advance notice, to meet the needs of the organization.				

JOB SUMMARY

The Information Security Analyst plays a critical role in safeguarding the organization's information systems, networks, and data. Reporting to the HCP AVP for Enterprise Operations, and Information Security Manager for day-to-day operations, this role supports cybersecurity initiatives and ensures compliance with HIPAA and other relevant regulations. The analyst will monitor security systems, assist with risk assessments, and enhance the organization's security posture by collaborating with IT teams to identify and address security threats.

ESSENTIAL JOB FUNCTIONS

- Maintain and support privacy and security programs aligned with NIST and HIPAA guidelines.
- Implement and monitor security controls across networks and systems.
- Collaborate with IT operations to ensure security measures are effectively deployed and maintained.
- Monitor security events and vulnerabilities; escalate issues as necessary.
- Escalate complex security issues to the Information Security Manager for further investigation.
- Conduct periodic risk assessments and audits under the direction of the Information Security Manager.
- Develop and maintain documentation for security policies, procedures, and incident response plans.
- Participate in security awareness training initiatives.
- Support incident response activities, including documentation and coordination with internal teams.
- Stay updated on evolving cybersecurity threats and industry trends through continuous learning.
- Assist with security risk assessments, vendor reviews, and remediation efforts.

- Monitor and investigate email filtering systems for potential threats.
- Analyze DMARC, DKIM, and SPF logs to enhance email security.
- Support cybersecurity training programs, phishing simulations, and user awareness initiatives.
- Respond to Tier 1 security-related support tickets and assist with account management tasks.
- Lead account removals and password manager account setups.
- Assist in cybersecurity awareness communications and best practices.
- Continuously monitor security alerts and logs within the environment.
- Perform initial triage of security alerts to assess severity and impact, distinguishing false positives from legitimate incidents.
- Execute basic incident handling procedures.
- Accurately and comprehensively document security incidents for analysis and reporting.
- Perform other duties and projects as assigned.

QUALIFICATIONS

Skills

- Understanding of HIPAA, HITECH, and general cybersecurity principles.
- Strong written and verbal communication skills.
- Ability to troubleshoot security-related issues and collaborate with cross-functional teams.
- Ability to work independently and in a remote environment.
- Strong attention to detail and organizational skills.
- Analytical thinking and problem-solving ability.
- Willingness to learn and adapt to new security technologies.

Technical Knowledge (Preferred)

- Familiarity with cloud platforms such as Office365, Azure AD, or AWS.
- Exposure to security tools including antivirus software, vulnerability scanners, and SIEM platforms
- Understanding of email encryption, endpoint protection, and forensic tools.
- Experience with IT ticketing systems or change management tools is a plus.

Education/Experience

- 4+ years of experience in an IS/IT environment required, preferably working as an IT Security Analyst or IT Compliance Analyst
- Experience in a healthcare environment is preferred.
- Working knowledge of IT risk management and compliance frameworks is a plus.
- Relevant certifications such as Security+, CySA+, SSCP, or equivalent are desirable.

Geographical Location, Standard Business Hours, and Travel Requirements

- Located in the assigned territory no more than a 60-minute radius to a major U.S. airport.
- Business hours are generally 8:00-5:00 PST.
- A minimum of 5% travel is required for staff development purposes.

PHYSICAL REQUIREMENTS

- Ability to sit or stand for long periods of time
- Ability to reach, bend and stoop

- Physical ability to lift and carry up to 20 lbs.

HIPAA/COMPLIANCE

- Maintain privacy of all patients, employee and volunteer information and access such information only on as need to know basis for business purposes.
- Comply with all regulations regarding corporate integrity and security obligations. Report Unethical, fraudulent, or unlawful behavior or activity.
- Upon hire and annually attend HCP's HIPAA training and sign HCP's Confidentiality & Non-Disclosure Agreement and HIPAA Privacy Acknowledgment
- Upon hire and annually read and acknowledge understanding of HCP's HIPAA Security Policies and Procedures
- Adhere to HCP's HIPAA Security Policies and Procedures and report all security incidents to HCP's Privacy & Security Officer

To express interest in this role, please submit your resume and application to jobs@hcpsocal.org.