CALHR
CALIFORNIA DEPARTMENT OF HUMAN RESOURCES

Duty Statement

Department of Human Resources

State of California

☐ Current ☒ Proposed

Classification Title	Division/Unit
Information Technology Specialist II	Information Technology Division / Infrastructure
Working Title	**HQ Designation**
Lead Infrastructure Security Engineer	CalHR Sacramento
Position Number	**Date Prepared**
363-175-1414-014	07/14/2026
Name	**Effective Date**

CalHR Mission, Vision, and Values

The California Department of Human Resources (CalHR) is responsible for issues related to employee salaries and benefits, job classifications, civil rights, training, exams, recruitment and retention. For most employees, many of these matters are determined through the collective bargaining process managed by CalHR.

Our Mission: To serve as the trusted advisor to our strategic partners and the public, providing exceptional human resource services and guidance in developing a diverse and inclusive workforce.

Our Vision: Shaping California's future of public service excellence with fair and equitable employment opportunities and a diverse, engaged workforce.

CalHR Core Values: People Centric, Leadership, Accountability, DEIA, Integrity, and Transparency.

General Statement

Under the direction of the Information Technology Manager I, Department of Human Resources (CalHR), Infrastructure Unit, the Information Technology Specialist II serves as a senior technical resource responsible for designing, implementing, securing, and maintaining enterprise infrastructure supporting CalHR's business operations. The incumbent provides advanced technical expertise across cloud environments, servers, storage, networking, directory services, and infrastructure security.

The incumbent leads and participates in complex infrastructure and security projects; provides technical analysis and recommendations; develops and implements secure, reliable, and scalable technology solutions; and supports the ongoing optimization of CalHR's infrastructure environment. The incumbent serves as a technical resource to staff and stakeholders, provides technical guidance and mentorship to junior staff, and establishes and maintains effective working relationships with customers, management, service providers, and other state agencies and departments.

The incumbent performs complex technical assignments involving infrastructure architecture, cloud and server administration, network and storage engineering, security, automation, disaster recovery, and operational support. The position requires the ability to analyze complex technical issues, develop innovative solutions, manage competing priorities, and apply current

industry standards and security practices to support CalHR's enterprise technology environment.

Job Functions

[Essential (E) / Marginal (M) Functions] conducted [Onsite (O) / Virtually (V)]:

Percentage	(O) / (V)	Essential Job Duties
30%	OV	**Cloud Security & Infrastructure Engineering** • Design, implement, and manage secure Microsoft Azure cloud architectures and resources, ensuring alignment with enterprise-level cloud landing zones, CalHR business needs, and state security frameworks. • Implement robust Cloud Security Posture Management (CSPM) and Identity and Access Management (IAM) controls, utilizing Azure Active Directory/Entra ID to manage role-based access control (RBAC), multi-factor authentication (MFA), and conditional access policies. • Monitor, detect, and respond to security threats within the cloud environment utilizing cloud-native security tools, specifically Microsoft Defender for Cloud and Microsoft Sentinel. • Engineer and configure secure, automated cloud deployments using Infrastructure as Code (IaC) and automation templates, integrating security guardrails directly into the deployment pipeline. • Perform security hardening, continuous monitoring, and configuration audits of cloud resources, storage accounts, virtual networks, and cloud-native databases to prevent misconfigurations, data exposure, and security drift. • Establish, enforce, and report on cloud compliance, logging, and audit trails to align cloud environments with CalHR, California Department of Technology (CDT), and Information Security Office policies.
20%	OV	**Server Architecture & Implementation** • Perform the most complex server configurations including, but not limited to, automated build templates, virtual server build templates, load balancing, Host Bus Adapter (HBA) configurations, Storage Area Network (SAN) integration (both bare-metal and virtual servers), performance baselining, and monitoring. • Create and implement system procedures based on security policies established by the Information Security Office, ensuring that all server configurations adhere to security best practices, state standards, and compliance baselines. • Design and configure highly available systems using clustering, multi-pathing, and other fault tolerance mechanisms, ensuring robust disaster recovery options. • Implement secure server designs with a focus on operating system hardening (Windows Server 2016+, Linux, and VMware), including the deployment, installation, and configuration of critical security patches and updates.

		• Maintain securely configured Demilitarized Zone (DMZ) infrastructures and hybrid network connections to Microsoft Azure to safely and securely offer services to CalHR customers. • Develop and maintain advanced shell scripts (e.g., PowerShell, Bash) to automate server administration, cloud resource provisioning, security auditing, configuration management, and patching workflows.
15%	OV	**Server Applications & Directory Services** • Design, implement, and maintain enterprise-level directory services and infrastructure, including Microsoft Active Directory, DNS, DHCP, Group Policy Objects (GPOs), and certificate management to ensure secure, resilient authentication and authorization mechanisms. • Configure and secure server applications, including Internet Information Services (IIS) and Network Policy Server (NPS), ensuring protection against system vulnerabilities and alignment with organizational security policies. • Manage and secure remote access applications (such as Citrix XenApp) with a focus on enforcing secure end-user access, encryption, and multi-factor authentication controls. • Maintain and support secure enterprise collaboration and messaging systems, implementing transport encryption, anti-spam, and anti-malware security configurations.
15%	OV	**Network Architecture & Security** • Perform configuration, optimization, and maintenance of networking equipment, including Palo Alto Firewalls, Cisco switches, wireless controllers, and access points, focusing on securing traffic, virtual networks, and micro-segmentation. • Manage the Forescout Network Access Control (NAC) system and integrate network-level security with hybrid, client-to-server, and cloud-connected security architectures. • Apply, monitor, and tune active security measures such as Intrusion Prevention Systems (IPS), Virtual Private Networks (VPNs), Web Filtering, and Data Loss Prevention (DLP) to maintain a highly defended enterprise network perimeter. • Create and implement network security procedures based on Information Security Office policies, ensuring all network baselines are secure, compliant, and audit-ready.
10%	OV	**Storage Engineering** • Perform advanced storage designs and maintenance of enterprise storage arrays and secure cloud storage repositories with an emphasis on data integrity, high availability, and confidentiality. • Manage Fibre Channel (FC) protocols, RAID levels, storage switches, and optimize SAN performance while configuring storage encryption-at-rest, secure access controls, and data retention policies.

		• Monitor, analyze, and predict storage performance trends, capacity limits, and data growth to proactively recommend security, encryption, and efficiency enhancements to the infrastructure team.
5%	OV	**Maintain and Develop Technical Expertise** • Serve as a technical mentor to junior system engineers, help desk staff, and business units to ensure effective succession planning and the secure, efficient operation of IT and cloud environments. • Attend trainings, webinars, and technical seminars to remain proficient in evolving cloud security paradigms, emerging cyber threats, and enterprise system administration best practices.
Percentage	**(O) / (V)**	**Marginal Job Duties**
5%	OV	**Non-Essential or Marginal Functions** • Perform other job-related duties as required, including representing the IT Infrastructure unit at division meetings, cross-functional workshops, or collaborative IT committees.

Supervision Received

The Information Technology Specialist II reports directly to and receives the majority of assignments from the Information Technology Manager I; however, direction and assignments may also come from CIO, CTO or other leaders in the division.

Supervision Exercised

None

Special Requirements/Desirable Qualifications

- Cloud Security Expertise: Advanced, hands-on experience designing, securing, and managing Microsoft Azure environments, with specific expertise in Cloud Security Posture Management (CSPM), Microsoft Defender for Cloud, Microsoft Sentinel, and Identity and Access Management (IAM/Entra ID).
- Enterprise Infrastructure & Operating Systems: Deep technical knowledge and experience configuring, hardening, and maintaining enterprise-level Windows Server (2016+), Linux, and VMware virtualization environments.
- Network & Perimeter Security: Proficiency with configuring, optimizing, and troubleshooting Palo Alto Firewalls, Cisco switches, and Network Access Control (NAC) systems like ForeScout.
- Storage Area Networks (SAN): Experience engineering and managing enterprise storage arrays, optimizing Fibre Channel protocols, and implementing storage encryption and data retention policies.
- Automation & Orchestration: Strong experience developing advanced automation scripts (e.g., PowerShell, Bash, or Infrastructure as Code) to streamline deployments, patching, and security audits.
- Analytical & Problem-Solving Skills: Excellent analytical, critical thinking, and troubleshooting skills, with the ability to resolve complex, high-priority technical issues under pressure.
- Professional Dependability & Communication: Exceptional written and verbal communication skills, a strong sense of accountability, and the ability to build collaborative relationships with teammates, stakeholders, and control agencies.

- Lead & Mentorship Experience: Demonstrated experience serving as a technical lead, steering complex IT projects, establishing technical standards, and mentoring junior systems engineers and technical staff.

Industry Certifications (Highly Desired): Possession of relevant industry-recognized certifications, such as:

- Certified Information Systems Security Professional (CISSP)
- Certified Cloud Security Professional (CCSP)
- Microsoft Certified: Azure Security Engineer Associate (AZ-500)
- Palo Alto Networks Certified Network Security Engineer (PCNSE)

CalHR employees are expected to model and support CalHR Core Values.

Working Conditions

The duties of this position are performed indoors at the 1515 “S” Street building. The employees’ workstation is equipped with standard or ergonomic office equipment, as appropriate.

To promote collaboration, team cohesion, and employee development, CalHR operates on a hybrid schedule in accordance with both Statewide and CalHR’s Telework Policies.

Attendance

Employees must maintain regular and acceptable attendance, as determined solely by the Department. They must be regularly available on-site or virtually and willing to work the hours deemed necessary or desirable to meet the Department's business needs.

Employee Acknowledgement

I have read and understand the duties listed above and I can perform these duties with or without reasonable accommodation (RA). * (If you believe an RA is necessary, discuss your concerns with the hiring supervisor. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will discuss your concerns with the RA Coordinator.)

*****An RA is any modification or adjustment made to a job, work environment, or employment practice or process that enables an individual with a disability or medical condition to perform the essential functions of their job or to enjoy an equal employment opportunity.

Duties of this position are subject to change and may be revised as needed or required.

Employee Signature	**Employee Name**	**Date**

I have discussed the duties of this position with and have provided a copy of this duty statement to the employee named above.

Supervisor Signature	**Supervisor Name**	**Date**