 **Security Engineer IV Standard Job Description**

**Classification Title:** Security Engineer IV

**FLSA Exemption Status:** Exempt

**Pay Grade:** 80

**Job Description Summary:**

The Security Engineer IV, under direction, provides leadership and oversight of the planning and designing of security solutions and capabilities that enable the organization to identify, protect, detect, respond, and recover from cyber threats and vulnerabilities.

**Essential Duties and Tasks:**

**50% Solutions Engineering**

* ​​​Leads the development and management of data, system, and network security architecture.
* Leads the implementation of new technology deployments and integration testing.
* Oversees the evaluation of security products, services, and procedures to enhance productivity and effectiveness.
* Provides leadership and mentors junior engineers in event management, data loss prevention, intrusion prevention systems, and enacting other security solutions.
* Oversees the design of action plans for policy creation and governance, system hardening, monitoring, incident response, disaster recovery, and emerging cybersecurity threats.

**20% Strategic Collaboration & Partnerships**

* ​​​Oversees the collaboration with enterprise stakeholders to coordinate the development of specifications within service-based solutions.
* Serves as head resource for other teams or organizations.
* Advises technical staff, policy administrators, and clients on the integrity of security procedures, systems, and policies in the design of systems and facilities.​​

**15% Security Analysis**

* ​​​Oversees, enforces, audits, and consults on the appropriate application of security policies and procedures.
* Administers and monitors data security on various platforms, conducts audits, reviews security violation reports, and investigates security exceptions.
* Oversees reporting in internal investigations of possible security violations.
* Oversees the review of documentation and logs of information security incidents, responses, plans, methods, and procedures.
* Oversees the defining and development of security requirements and assessing of existing systems.
* Keeps abreast of the latest intelligence for cyber threat information.

**10% Documentation**

* ​​Oversees the development of standard operating procedures.
* Oversees documentation provided to partner support teams, customers, stakeholders, and vendors.
* Oversees the creation and maintenance of documentation for technologies, including installation, configuration, and appropriate troubleshooting steps.​​

**5% Professional Development**

* ​​​Participates in training, professional development sessions, and continual and ongoing training and exploration into new technologies.​​

**Qualifications**

**Required Education:**

* Bachelor’s degree or an equivalent combination of education and experience.

**Required Experience:**

* Eight years of related experience in information technology security operations.

**Required Licenses and Certifications:**

* None

**Required Knowledge, Skills, and Abilities:**

* Ability to multitask and work cooperatively with others.
* Broad IT technical knowledge.
* Ability to analyze and solve complex problems.
* Excellent written communication, interpersonal, and organizational skills.

**Preferred Qualifications:**

* Experience building security tools & platforms for large enterprise environments
* Knowledge of security tools like SIEMs, firewalls, vulnerability scanners, and intrusion detection systems
* Ability to identify security incidents, anomalies, and vulnerabilities
* Scripting experience of some kind (Python, Bash, Powershell, etc)
* Knowledge of security best practices and ability to conduct risk assessments, audits, and tests
* Understanding of frameworks like ISO 27001, NIST CSF, NIST 800-53 and 800-171, CIS controls, etc
* Familiarity with regulatory frameworks such as HIPAA, FERPA, GLBA, TAC 202, TGC 2054, etc
* Hands-on technical expertise, knowledge of security frameworks and policies, and analytical thinking. Soft skills like communication, collaboration, and the ability to translate technical details for non-technical audiences are also key for this role.

**Additional Information**

**Machines and Equipment:**

* Computer
* Phone

**Physical Requirements:**

* None

**Other Requirements and Factors:**

* Hiring restrictions in compliance with System Policy 15.02 Export Controls: Must be a United States citizen, permanent resident, or a person granted asylum or refugee status in accordance with 15 CFR, Part 762; 22 CFR §§122.5, 123.22 and 123.26; and 31 CFR § 501.601.
* This role may require working outside of standard office hours, including evenings, weekends, and holidays, to support the demands of technology services and ensure the seamless operation of essential systems.
* This position is security sensitive.
* This position requires compliance with state and federal laws/codes and Texas A&M University System/TAMU policies, regulations, rules and procedures.
* All tasks and job responsibilities must be performed safely without injury to self or others in compliance with System and University safety requirements.

**Is this role ORP Eligible? If so, it needs to meet the criteria on the** [**Rules and Regulations of the Texas Higher Education Coordinating Board**](https://reportcenter.highered.texas.gov/reports/data/user-friendly-version-of-ch-25/)**.**

**Yes**

**No**

**Does this classification have the ability to work from an alternative work location?**

**Yes**

**No**