 **Security Analyst II P70 Standard Job Description**

**Classification Title:** Security Analyst II P70

**FLSA Exemption Status:** Exempt

**Pay Grade:** 70

**Job Description Summary:**

The Security Analyst II P70, under general direction, performs complex and non-routine specialized information technology (IT) security analysis functions, such as troubleshooting, advanced analysis, research, and problem-solving.

**Essential Duties and Tasks:**

**40% Security Analysis**

* ​​​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.
* Conducts and reports on internal investigations of possible security violations.
* Reviews the accuracy of documentation and logs of information security incidents, responses, plans, methods, and procedures.
* Develops risk analysis scenarios and response procedures.

**20% Solutions Engineering**

* ​​​Develops and manages data, system, and network security architecture.
* Implements new technology deployments and integration testing.
* Evaluates security products, services, and procedures to enhance productivity and effectiveness.
* Assists project leaders with developing work plans and time schedules for projects including outlining phases and identifying personnel and computing equipment requirements.

**20% Strategic Collaboration & Partnerships**

* ​​​Collaborates with enterprise stakeholders to coordinate the development of specifications within service-based solutions.
* Serves as a 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.

**10% Documentation**

* ​​​Develops standard operating procedures.
* Coordinates documentation provided to partner support teams, customers, stakeholders, and vendors.
* Create and maintain documentation for technologies, including installation, configuration, and appropriate troubleshooting steps.

**10% 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 equivalent combination of education and experience.

**Required Experience:**

* Three years of security analysis or development experience.

**Required Licenses and Certifications:**

* None

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

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

**Preferred Qualifications:**

* Knowledge of security best practices and ability to conduct risk assessments, audits, and tests
* Knowledge of security tools like SIEMs, firewalls, vulnerability scanners, and intrusion detection systems
* Ability to identify security incidents, anomalies, and vulnerabilities
* 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
* Scripting experience of some kind (Python, Bash, Powershell, etc)
* The ideal candidate will have a blend of 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**