



TEXAS WOMAN'S
UNIVERSITY™

DATE ISSUED: 08/15
FLSA: Exempt
PTO: VCS

JOB DESCRIPTION

TITLE

Data Security Analyst

JOB SUMMARY

The Data Security Analyst performs two core functions for the enterprise. The first is the day-to-day operations of the in-place security solutions while the second is the identification, investigation and resolution of security breaches detected by those systems. Secondary tasks may include involvement in the implementation of new security solutions, participation in the creation and or maintenance of policies, standards, baselines, guidelines and procedures as well as conducting vulnerability audits and assessments. The Data Security Analyst is expected to be fully aware of the enterprise's security goals as established by its stated policies, procedures and guidelines and to actively work towards upholding those goals. Work is performed under general supervision and the performance is based upon completion of assignments and results obtained. The performance evaluation is conducted through the performance evaluation system and in accordance with the University Policies & Procedures.

ORGANIZATIONAL RELATIONSHIPS

Reports to: Information Security Manager

Supervises: As assigned

ESSENTIAL DUTIES - May include, but not limited to the following:

- Participates in the planning and design of enterprise security architecture, under the direction of the Information Security Manager, where appropriate.
- Participates in the creation of enterprise security documents (policies, standards, baselines, guidelines and procedures) under the direction of the Manager of Information Security, where appropriate.
- Participates in the planning and design of an enterprise Business Continuity Plan and Disaster Recovery Plan, under the direction of the Manager of Information Security, where appropriate.

- Maintains up-to-date detailed knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the development of new attacks and threat vectors.
- Recommends additional security solutions or enhancements to existing security solutions to improve overall enterprise security.
- Performs the deployment, integration and initial configuration of all new security solutions and of any enhancements to existing security solutions in accordance with standard best operating procedures generically and the enterprise's security documents specifically.
- Maintains up-to-date baselines for the secure configuration and operations of all in-place devices, whether they be under direct control (i.e., security tools) or not (i.e., workstations, servers, network devices, etc.).
- Maintains operational configurations of all in-place security solutions as per the established baselines.
- Monitors all in-place security solutions for efficient and appropriate operations.
- Reviews logs and reports of all in-place devices, whether they be under direct control (i.e., security tools) or not (i.e., workstations, servers, network devices, etc.). Interpret the implications of that activity and devise plans for appropriate resolution.
- Participates in investigations into problematic activity.
- Participates in the design and execution of vulnerability assessments, penetration tests and security audits.
- Provides on-call support for end users for all in-place security solutions.

ADDITIONAL DUTIES

- Performs other duties as requested.

EDUCATION

Bachelor's degree required. Additional job related experience/and/or education may substitute for the required education on a year-for-year basis. CISSP certification preferred.

EXPERIENCE

Three years job related work in computing and/or communications, education environment highly preferred.

REQUIREMENT

Regular and reliable attendance at the University during regular scheduled days and work hours is an essential function of this position.

KNOWLEDGE, SKILLS, AND ABILITIES - *The following are essential:*

Knowledge:

- The theories, principles, practices, methods, and techniques used in the field of information security and network management.
- Troubleshooting techniques for electronic equipment and systems.
- Quality assurance concepts and procedures.
- Strong understanding of IP, TCP/IP, and other network administration protocols.
- Experience in enterprise security architecture design.
- Experience in enterprise security document creation.
- Experience in designing and delivering employee security awareness training.
- Experience in developing Business Continuity Plans and Disaster Recovery Plans.

Skills Required:

- Security Testing and Auditing
- Security Risk Management
- Network Security Management
- Methods for cost estimation and risk analysis
- Prototyping procedures
- Requirements gathering
- Conflict Resolution
- Financial Analysis
- Strong interpersonal, written, and oral communication skills.
- Ability to present ideas in user-friendly language.
- Highly self-motivated and directed, with keen attention to detail.
- Proven analytical and problem-solving abilities.
- Able to effectively prioritize tasks in a high-pressure environment.
- Strong customer service orientation.
- Experience working in a team-oriented, collaborative environment.
- Strong technical documentation skills.
- Good interpersonal skills.
- Project management software tools
- Risk analysis

Ability to:

- Operate on independent judgment based on an understanding of organizational policies and activities.
- Establish and maintain effective work relationships with students, faculty, staff, and the public. Communicate effectively orally, by phone, in person, and in writing.
- Represent the department and University in a friendly, courteous, and professional manner.
- Use a personal computer and other office equipment, including university related software and email.

PHYSICAL DEMANDS

The physical demands described in the Essential Duties and below are representative of those that must be met by an employee to successfully perform the essential duties of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential duties.

The employee may be required to travel.

WORK ENVIRONMENT

All employees are responsible for maintaining an environment that is free from discrimination, intimidation, harassment, including sexual harassment. Work is normally performed in a typical interior work environment.

SAFETY

TWU promotes a safe working environment. Employees are responsible for completing assigned tasks safely and efficiently, and supervisors are responsible for creating and maintaining a safe work environment. Employees must report any unsafe work conditions or practices, as well as any near-miss incidents, to their supervisor and Risk Management. Supervisors and employees should ensure that injury/accident reports are submitted to the Office of Human Resources and Risk Management within 24 hours of the incident.

The job description does not constitute an employment agreement between the employer and employee and is subject to change by the employer as the needs of the employer and requirements of the job change.

Employee Signature: _____ **Date:** _____

Employee Printed Name: _____

Texas Woman’s University strives to provide an educational environment that affirms the rights and dignity of each individual, fosters diversity, and encourages a respect for the differences among persons. Discrimination or harassment of any kind is considered inappropriate.

Texas Woman’s University is committed to equal opportunity in employment and education and does not discriminate on the basis of race, color, religion, gender, sex,

*Data Security Analyst
Date Issued: 08/15
FLSA: Exempt
PTO: VCS*

sexual orientation, ethnic origin, age, veteran's status, or against qualified disabled persons.

All positions at Texas Woman's University are deemed security sensitive requiring background checks.