# PUBLIC UTILITY COMMISSION OF TEXAS
# JOB DESCRIPTION

| | | | |
|---|---|---|---|
| **Classified Title:** | Information Security Analyst II - III | **Class Code:** | 0236, 0237 |
| **Working Title:** | IT Security Analyst | **Salary Group:** | B25, B27 |
| **Division:** | Agency Operations | **FLSA:** | Exempt |
| **Supervisor:** | IT Manager | **Date:** | 05/19/23 |

## GENERAL DESCRIPTION:

Perform highly complex to advanced computer information security analysis work. Work involves overseeing and planning, implementing, and monitory security measures for the protection of information systems and infrastructure. Work under limited to minimal supervision with considerable to extensive latitude for the use of initiative and independent judgment.

## ESSENTIAL FUNCTIONS:

- Oversee and perform the design, automation, and deployment of security applications and infrastructure program activities.
- Oversee and implement computer system security plans with PUC staff.
- Develop and/or coordinate the development of agency policies for encryption of data transmissions and the definition of firewall configuration to protect confidential information in transit.
- Develop, recommend, and implement plans to safeguard computer configuration and data files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Develop information technology disaster recovery and business continuity planning for the PUC technology infrastructure. Advises management and users regarding security configurations and procedures.
- Perform and review technical risk assessments; reviews of new and existing applications and systems, including data center physical security and environment; and reviews of account permissions, computer data access needs, security violations, and programming changes.
- Modify and monitor computer configuration and data files to incorporate new software and virus protection systems, correct errors, or change individual access status.
- Design and plan deployment of continuous automated security compliance capabilities.
- Monitor and evaluate systems and procedures to protect data systems and databases from unauthorized access.
- Research, evaluate, and recommend systems and procedures for the prevention, detection, containment, and correction of data security breaches.
- Train users and promote security awareness to ensure system security and to improve application, server, and network efficiency.
- Serve as a primary backup to the agency DCS Customer Representative.
- Assist in resolving performance issues relating to the State Data Center and the PUC network.
- May plan, assign, and supervise the work of others.
- Demonstrate a spirit of teamwork, offering positive and constructive ideas, encouragement, support to other members of the staff and team, and respond professionally to constructive feedback from others, while upholding the PUC's mission and core values.
- Adhere to all agency personnel policies and division procedures and perform other work as assigned

## REQUIRED MINIMUM QUALIFICATIONS:

Information Security Analyst II: Graduation from an accredited college or university with major course work in information technology security, computer science, computer information systems or management information systems, or a related field **and** three (3) years' experience working in the IT security industry. ***Relevant full-time work experience may substitute for education on a year per year basis.***

Information Security Analyst II: Graduation from an accredited college or university with major course work in information technology security, computer science, computer information systems or management information systems, or a related field **and** five (5) years' experience working in the IT security industry. ***Relevant full-time work experience may substitute for education on a year per year basis***

## PREFERRED QUALIFICATIONS:

Experience working with state IT regulatory issues and processes.
Experience and training in analyzing, recommending, developing, and implementing cogent enterprise-wide policies, standards, and guidelines.
Have or working towards obtaining a Certified Information Systems Security Professional (CISSP) Or similar certification.

## KNOWLEDGE, SKILLS AND ABILITIES:

Must possess required knowledge, skills, abilities, and experience and be able to explain and demonstrate, with or without accommodations, that the essential functions of the job can be performed.

- Ability to analyze systems and processes; to write and revise standards and procedures; to handle multiple projects; to communicate effectively; and to plan, assign and/or supervise the work of others.
- Knowledge of the limitations and capabilities of computer systems; technology across all mainstream network, operating system, and application platforms; operational support of networks, operating systems, Internet technologies, databases, and security applications; and information security practices, procedures, and regulations.
- Skill in the use of applicable software and the configuring, deploying, monitoring, and automating of security applications and infrastructure.
- Ability to resolve complex security issues in diverse and decentralized environments; to learn, communicate, and teach new information and security technologies; to communicate effectively; and to supervise the work of others.
- Ability to attend work regularly and adhere to approved work schedule.

## TELECOMMUTING ELIGIBILITY:

- This position is eligible for telecommuting up to three (3) days a week but may require team members to come into the office for scheduled meetings, and there may be unscheduled requests with appropriate notice for any PUC business need.
- If approved to telecommute, must have a secure workspace with reliable Internet service to perform duties, ability to maintain a reliable consistent work schedule and be available for weekly meetings and group collaboration via Microsoft Teams and other applications during regular business hours.

## PHYSICAL AND COGNITIVE REQUIREMENTS AND WORKING CONDITIONS:

The physical and cognitive demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations will be made if needed to enable individuals with disabilities to perform the essential functions.

This position primarily performs sedentary office work. It requires extensive use of computer, copiers, printers, telephone and requires communication with staff and the public. This position also requires cognitive abilities consistent with the essential functions and with the knowledge, skills and abilities; requiring the ability to learn, recall, and apply practices and policies. It requires the stamina to maintain attention to detail despite interruptions.

Work is performed in a standard office environment or secure telework space and requires:

- Regular and punctual attendance.
- Frequent use of personal computer, copiers, printers and telephones.
- Frequent sitting.
- Frequent work under deadlines, as a team member, and in direct contact with others.
- Occasional moving and lifting objects up to 10 pounds.

**PUBLIC UTILITY COMMISSION OF TEXAS**
**JOB DESCRIPTION ACKNOWLEDGMENT**

**INFORMATION SECURITY ANALYST** is an at-will employment position. It is, therefore, employment for no specified term of months or years, not under contract, and able to be terminated by the employee or the Public Utility Commission of Texas (PUCT) at any time for any reason other than those prohibited by state and federal law. The PUCT may use a system of progressive discipline prior to or instead of termination, but it is not required to do so.

The information provided below is not to be considered a contract. Its primary purpose is to provide an inclusive job description for the position of **INFORMATION SECURITY ANALYST** of the PUCT. It is also intended to provide background information to any member of the general public regarding the duties of **INFORMATION SECURITY ANALYST**.

An employee, by signing below, acknowledges that he or she has read the entire job description and understands the nature of at-will employment and the duties of the position.

SIGNATURES: (*Please sign and return the signed job description and the electronic file to Human Resources.)*

_____ _____
Employee Name (Print) Date

_____
Employee Signature