# COUNTY OF HIDALGO
## Department of Human Resources

Job Title: **CYBERSECURITY ANALYST I**
Grade: 10

*The County of Hidalgo Department of Human Resources reserves the right to select candidates considered to be the most highly qualified based on education and experience. The hiring department will interview and select the candidates provided by the Department of Human Resources.*

**GENERAL DESCRIPTION**

Individual is tasked with complex (journey-level) security of the information contained within the County's network infrastructure and related systems and peripherals. Responsible for analyzing and safeguarding security controls for all systems.

**EXAMPLES OF WORK PERFORMED**

Ensure timely response and management of any cyber incident to minimize risk exposure and production down time.

Conduct incident response activities, including advanced investigation to investigate potential security incidents.

Safely acquire and preserve the integrity of cyber security data required for incident analysis to help determine the technical/operational impact, root cause(s), scope and nature of the incident.

Analyze and correlate incident data to develop a preliminary root cause and corresponding remediation strategy.

Evaluate target systems to analyze results of scans, identify, and recommend resolutions.

Utilize incident response playbooks to follow established and repeatable processes for triaging and containment of an incident.

Investigate and resolve cyber security incidents.

Routinely develop and update incident response to activities align with best practices, minimize gaps in response and provide comprehensive mitigation of threats.

Provide timely, comprehensive, and accurate information to IT Director in both written and verbal communications.

Experience in data security standards as it relates to user accounts and access

Comprehensive knowledge of databases, scripts and queries

A solid grounding in IT fundamentals such as web applications, and system administration.

Design firewalls, monitor use of data files, and regulate access to safeguard information and protect the network.

Staying up to date on current virus reports and protecting networks from viruses.

Installing and running protective software, such as data encryption programs and firewalls.

Requires the ability to apply principles of logical or scientific thinking to define problems, collect data, establish facts and draw valid conclusions; to interpret and extensive variety of technical instructions in mathematical or diagrammatically form; and to deal with several abstract and concrete variables

Maintains accurate computer inventory and location of all computer software and hardware including peripherals; Task includes installing and de-installing systems and maintaining accurate software licensing and information

Works with the Network Administrator to coordinate software and hardware inventory for the County

Assembles hardware and/or software components, performs hardware/software integration to provide a stand-alone computer system, and ensures it is operating as it is designed and operates properly

Configures and installs PCs and related software and set up and configure network connections to file servers, application servers and the Internet

Coordinates deliveries and installation of equipment to user installations and performs tests to ensure the system is operating properly, de-installs equipment and provides replacement system as required

Works with vendors to resolve non-functioning equipment problems arranging for replacements and/or exchanges

Supervise and train co-workers and assistants on daily duties and during projects

Performs all other related duties as assigned

**EXPERIENCE AND EDUCATION**

Bachelor's Degree in Cyber Security/ Computer related field

One (1) year of experience as a high level cyber security analyst.

Must have at least three (3) years' experience in the information technology field

Two (2) years of related experience may be substituted for one (1) year of education

Other IT certifications are preferred

Good understanding and knowledge of computer systems is required with knowledge of mainframe systems, related software, business principles and procedures

**CERTIFICATES, LICENSES AND REGISTRATION**

Certification in one or more of the following preferred:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- CompTIA Security+
- Certified Ethical Hacker (CEH)

- GIAC Security Essentials (GSEC)

Must have a current valid Texas motor vehicle operator's license

Must be able to be insured by the County's insurance carrier

**KNOWLEDGE, SKILLS AND ABILITIES**

Good understanding and knowledge of computer systems is required

Requires the ability to research and comprehend emerging security threats

Requires the ability to develop and implement plans and procedures and maintain up-to-date security policies, standards, guidelines, and baselines.

Requires the ability to communicate and interact within the Technology Services team and with other county departments.

Ability to work independently or as part of a team, good oral and written communication skills, strong analytical and organizational skills, ability to solve problems quickly and completely and coordinate activities simultaneously

**PHYSICAL DEMANDS**

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job.

While performing the duties of this job, the employee is regularly required to talk or hear. The employee frequently is required to stand. The employee is occasionally required to walk; sit; use hands to find, handle, or feel objects, tools or controls; reach with hands and arms; climb or balance; stoop and kneel.

The employee must occasionally lift and/or move over twenty-five (25) pounds. Specific vision abilities required by this job include close vision, depth perception, and the ability to adjust focus.

**WORK ENVIRONMENT**

The work environment characteristics described here are representative of those an employee encounter while performing the essential functions of this job.

The noise level in the work environment is usually moderate.

**SAFETY REQUIREMENTS**

Maintain physical conditions appropriate to the performance of assigned duties and responsibilities which may include the following:

- sitting for extended periods of time
- standing for extended periods of time
- operating assigned equipment

Maintain mental capacity which permits:

- making sound decisions and using good judgment
- demonstrating intellectual capabilities

Effectively handle a work environment and conditions which involve:

- working closely with others

- working in a multi-task environment

Maintain effective audio-visual discrimination and perception needed for:

- making observations
- reading and writing
- operating assigned equipment
- communication with others
- required to follow the County of Hidalgo Accident Prevention Plan and department's safety regulations