COUNTY OF HIDALGO

Department of Human Resources

Job Title:	**SYSTEM SERVICES ADMINISTRATOR**
Grade:	16

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

Oversees the System Services and Cyber Security environments. Develops an action plan to optimize data center services by tracking performance, memory, storage, growth requirements for County applications and services. Develops an action plan for the security needs to protect the county's network by investigating and monitoring logs and network traffic to be in a proactive stance, addressing vulnerabilities, weakness, and strategies dealing with the security posture of the county. Provides budgetary plan for refresh and/or upgrades of data center and security environment. This position will be responsible for all facets of the assigned projects for Systems Services and Cyber Security environments.

EXAMPLES OF WORK PERFORMED

Manage information technology and computer systems

Plan, organize, control, and evaluate IT and electronic data operations

Supervise Data Center Project staff by training and coaching employees, communicating job expectations, and appraising their performance

Design, develop, implement, and coordinate systems, policies, and procedures

Ensure security of data, network, servers, and backup systems

Act in alignment with user needs and system functionality to contribute to organizational policy

Identify problematic areas and implement strategic solutions in time

Preserve assets, information security and control structures

Enforce company security policies

Assist other IT staff in various IT projects, as needed

Lead a team of Cyber Security Professionals in the delivery of superior Information Assurance (IA) services, to include filling gaps in coverage, development of process documentation, testing of various plans, leading simulated cybersecurity events and other training.

Assist with creation and modification of processes to meet Risk Management Framework (RMF) control requirements, including defining system security requirements, assessing system security architecture designs, and supporting the development and sustainment of an Enterprise RMF Accreditation package throughout all Authority to Operate (ATO) lifecycle phases.

Ability to research and implement cost effective, automated security solutions like Security Information Event Management (SIEM) and perform Security Impact Analysis (SIA) to determine the risk of changes to the information system.

Perform technical cyber security related planning and effectiveness analyses for the Information Technology (IT) infrastructure design.

Ensure Plan of Action & Milestone (POA&M) reports are maintained and that security vulnerabilities are tracked and remediated by integrating with the Engineering and System Admin teams to help harden and monitor system performance.

Conduct certification and testing in accordance with the Risk Management Framework (RMF) and National Institute of Standards and Technology (NIST) policy; identify deficiencies and provide recommendations of risk mitigation to customer.

Evening and weekend work is required

Performs such other duties as may be assigned

Regular attendance is a must

EDUCATION AND EXPERIENCE

Bachelor's Degree in Information Technology or related field

Must have at least seven (7) years' experience in the information technology field

Proficient in Microsoft Server Operating Systems

Experience with Active Directory (AD), Group Policy Objects (GPO's), Domain Named Services (DNS)

Experience with virtual environments

Experience with backup technologies

Knowledge and understanding of Information Assurance Policies, including:

- National Institute of Standards and Technology (NIST) SP 800-115, Technical Guide to Information Security Testing and Assessment
- NIST SP 800-53 Rev4, Security and Privacy Controls for Federal Information Systems and Organizations
- Defense Information Systems Agency (DISA) Connection Process Guide (CPG)

CERTIFICATES, LICENSES AND REGISTRATION

One or more Certifications Preferred (not required)

- Certified Ethical Hacker (CEH)
- CompTIA Security+
- Certified Information System Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- NIST Cybersecurity Framework (NCSF)
- Certified Cloud Security Professional (CCSP)

- Computer Hacking Forensic Investigator (CHFI)
- Cisco Certified Network Associate (CCNA) Security

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

Knowledge of industry standard computer hardware and software

Requires the ability to compare and/or judge the readily observable, functional, structural, or composite characteristics (whether similar to or divergent from obvious standards) of data, people or things

Knowledge of systems analysis techniques and procedures, including consulting with users, to determine hardware, software or system functional specifications, determine procurement requirements for systems and peripherals.

Perform software licensing, installations, configuration and troubleshooting.

Design, document, test, create and modify computer programs related to machine operating systems, and troubleshoot hardware, software, and network-related issues.

Support security incident reporting, vulnerability assessments, and information assurance compliance scans.

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

Employee may be assigned other duties in addition to those listed; duties may change according to the changing needs of the County

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