

Information Technology Administrator Job Description

Department: Information Technology

General Function:

The Information Technology Administrator is responsible for ensuring the integrity and security of all technology systems that support Washington County customers as well as end users. The IT Administrator is a key technical resource, providing advice, training and technical support for various projects and daily operations. This position works closely with the County Administrator in evaluating current systems and aligning county objectives with the County strategy for technology.

Major Job Duties and Responsibilities

Manage the deployment, monitoring, maintenance, development, upgrade, and support of all IT systems, including servers, PCs, operating systems, phones systems, mobile devices, telephone infrastructure, firewalls, network hardware, equipment, and software applications.

- Provide expertise and support during systems upgrades, installations, conversions, and file maintenance.
- Oversee system development and enhancement and the integration of new systems with existing systems.
- Develop standard operating procedures, training, and best practices, including providing written protocols and guidance to IT staff and to end-users.
- Keep current with the latest technologies and determine what new technology solutions and implementations will meet business and system requirements.
- Supervise and provide end-user services, including help desk and technical support services.
- Manage financial aspects of the IT Department, including purchasing, budgeting, and budget review.
- Responsible for compliance with HIPPA and CJIS regulations and is the point of contact for external auditors and examiners.
- Responsible for monitoring and oversight of daily, monthly, and quarterly reports from Network vendors.
- Develop and implement all IT policies and procedures in co-ordination with the County Administrator, including those for security, disaster recovery, purchasing, and service provision.
- Negotiate and administer vendor, outsource, and consultant contracts and service agreements in co-ordination with the County Administrator.
- Provide technical assistance, support, and troubleshooting in the resolution of system communications failures and conflicts.

- Review, prioritize, and process problem reports; document the progress of projects.
- Maintain system compliance with current security policies, patches, and procedures.
- Provide strategic planning information to the County Administrator and State of Colorado as needed.
- Leads Disaster Recovery efforts for IT. Ensures backup and recovery of data is made to prevent down time of necessary County services, software, and hardware is minimal.
- Perform other duties as assigned.

Knowledge, Skills, and Abilities

- Possess a strong background in the Windows OS and Windows Server OS. Advanced knowledge of a wide range of computer systems software, applications, hardware, networking, and communications.
- Ability to diagnose and rectify a wide range of complex computer hardware, software and network issues.
- Ability to communicate effectively, both orally and in writing.
- Knowledge of customer service standards and procedures. Possess strong interpersonal and communication skills and the ability to work effectively under stress.

Working Conditions and Physical Effort

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. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

- Be on-call as requested to work on evenings and weekends.
- Moderate physical activity. Requires handling of average-weight objects up to 60 pounds or standing and/or walking for more than two (2) hours per day.
- Little or very limited exposure to physical risk.

Minimum Job Requirements

- MCSA in Server 2012 R2, Server 2016 or Server 2019
- Must be proficient in SQL Server, IIS Server, Hyper-V Server, Sonicwall firewalls, Sonicpoint, Engenius and Cisco Access Points, Amcrest and Avigilon Surveillance Systems
- Current Network+ and Security+ Certificates recommended
- Cyber security experience mandatory with CIS top 20 framework preferred
- Experience with Avaya IP Office 500 V2 phone systems, and Avaya L3 switches recommended