MORRISON COUNTY

JOB DESCRIPTION

Job Title:	Security Manager
Department:	Information Technology
Classification:	9
Reports to:	Information Technology Director
Supervises:	Yes
Normal Business Hours:	Monday – Friday, 8:00 AM – 4:30 PM
Telecommute:	By exception
Union:	No
FTE Status:	1.0 Full Time Equivalent
Last Reviewed:	08/2024

Nature of Work:

This position is responsible for and manages the secure operation of the county's computer systems, servers, and network connections. This includes the day-to-day operations of the in-place security solutions along with checking server and firewall logs, scrutinizing network traffic, establishing, and updating virus scans, and troubleshooting. This position will analyze and provide direction and operational support to resolve security concerns and vulnerability issues in a timely and accurate fashion through management of the service desk staff.

Communicates with:

Internally – All staff.
Externally – Vendors, government agencies, and public.

Supervision:

IT Support Specialist
Help Desk Specialist

Essential Work Functions:

Strategy & Planning

- Participates in the planning, development, implementation, and oversee enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices with direction provided by the IT Director.
- Participates in the planning and design of an enterprise business continuity plan and disaster recovery plan, under the direction of the IT Director, where appropriate.
- Assess needs for any security reconfigurations and their execution.
- Conducts research on emerging products, services, protocols, and standards in support of security enhancement and development efforts.

Acquisition & Deployment

- Recommends additional security solutions or enhancements to existing security solutions to improve overall enterprise security.
- Recommends, schedules, and performs security improvements, upgrades, and/or purchases.
- 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.

Operational Management

- Manages and provides guidance to members of the IT service desk team.

- Monitors all in-place security solutions for efficient and appropriate operations.
- Reviews logs and reports of all in-place devices, whether they are under direct control (i.e. security tools) or not (e.g. workstations, servers, network devices). 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.
- Designs, implements, and reports on security system and end user activity audits.
- Monitors server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity. Interpret activity and make recommendations for resolution.
- Recommends, schedules (where appropriate), and applies fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach.
- Downloads and tests new security software and/or technologies.
- Performs tests on system backups with the System Administrator.
- Provides security support to end-users.
- Performs regular security awareness training for all employees to ensure consistently high levels of compliance with enterprise security documents.

Other Work Functions

- Performs related work as required.

Minimum Qualifications of Education and Experience:

- Associate degree with an emphasis in Cybersecurity.
- Minimum of 1 (one) year of experience in cybersecurity with recent, professional certifications or an equivalent combination of education and experience. Three years of recent experience specific to cybersecurity with professional certifications can substitute for the associate's degree.
- Preferred experience in management of staff.
- Ability to pass all position required background(s) and testing(s).

Knowledge, Skills, and Abilities Required:

- Broad hands-on knowledge of firewalls, intrusion detection systems, anti-virus software, data encryption, and other industry-standard techniques and practices.
- In-depth technical knowledge of network, PC, and platform operating systems.
- Working technical knowledge of current systems software, protocols, and standards such as NIST, CIS benchmarking.
- Strong knowledge of TCP/IP and network administration/protocols.
- Knowledge of applicable practices and laws relating to data privacy and protection.
- Knowledge of law enforcement practices and procedures relating to operations and security standards published by the FBI.
- Intuition and keen instincts to prevent attacks.
- High level of analytical and problem-solving abilities.
- Ability to conduct research into security issues and products as required.
- Strong understanding of the organization’s goals and objectives.
- Strong written, interpersonal, and oral communication skills for a variety of technical and non-technical audiences.
- Ability to follow data practices requirements regarding confidentiality and privacy.
- Ability to present ideas in business-friendly and user-friendly language.
- Highly self-motivated and directed.

- Strong organizational skills.
- Ability to work extended evening and weekend hours as needed.
- Excellent attention to detail.
- Ability to effectively prioritize and execute tasks in a high-pressure environment.
- Able to work in a team-oriented, collaborative environment.

Persons with disabilities:
The above is a general listing of job duties. Essential and non-essential functions may vary by individual position. Reasonable accommodation may be available for both essential and non-essential job duties.

Physical Demands and Work Environment:
In compliance with Americans with Disabilities Act, the following represents the Physical and Environmental Demands:

Exposed to:	**24% or Less**	**25% - 49%**	**50%-74%**	**75% or more**
Office environment				X
Sitting, standing			X	
Walking, reaching, pulling		X		
Typing/data entry			X	
Talking, hearing			X	
Close and distance vision		X		
Moderate (Over 60 pounds of force)	X			
Challenging or threatening behaviors	X			
Work with high detail/deadlines			X	

This document does not create an employment contract, implied or otherwise, other than an "at will" employment relationship. The Board of Commissioners, County Administrator and/or the Department Head retains the discretion to add duties or change the duties of this position at any time.

Morrison County is an Equal Opportunity Employer. In compliance with the Americans with Disabilities Act, the County will provide reasonable accommodation to qualified individuals and encourages both prospective and current employees to discuss potential accommodations with the employer.

Employee Name: _____

Employee Signature: _____ Date: _____