IT/6

Cybersecurity Analyst

Information Technology
FLSA: E
Established Date: January 5, 2026

JOB SUMMARY

The position is responsible for continuous monitoring, vulnerability management, incident response, policy development, and employee security awareness. The Analyst evaluates, strengthens, and maintains the County's security posture across all systems, networks, and applications to ensure compliance, reliability, and data integrity.

MAJOR DUTIES

- Monitors County networks, servers, and endpoints for vulnerabilities, threats, or breaches using SIEM and intrusion detection tools.
- Responds to alerts and incidents from firewalls, antivirus, email filters, and endpoint protection systems.
- Conducts vulnerability assessments, risk assessments, and authorized penetration testing activities to identify and mitigate security risks.
- Develops and maintains cybersecurity policies, standards, and procedures in alignment with CJIS, HIPAA, and NIST frameworks.
- Coordinates the modernization, maintenance, and periodic testing of the Incident Response Plan, Discovery Recovery Plan, Continuity of Operations Plan/Continuity of Government (COOP-COG), and recovery processes.
- Manages user access controls and enforces least-privilege principles across County systems.
- Monitors, configures, and maintains Countywide system auditing and logging to ensure comprehensive event tracking, compliance, and timely detection of anomalies or unauthorized activity.
- Researches, recommends, and assists in implementing/managing security technologies including firewalls, multifactor authentication, and encryption solutions.
- Supports cybersecurity aspects of election infrastructure and other critical systems.
- Helps coordinate Countywide cybersecurity awareness and training programs for all employees.
- Assists in tabletop exercises, business continuity and disaster recovery planning.
- Collaborates with IT staff, vendors, and department heads to assess risk, review contracts, and ensure vendor compliance with County security requirements.
- Prepares reports on incidents, vulnerabilities, and cybersecurity trends for the IT Director and Board of Supervisors as requested.
- Stays informed on emerging threats, tools, and regulatory changes affecting cybersecurity.
- Assists with County cybersecurity insurance requirements, assessments, and incident documentation as needed.
- Performs related duties as assigned.

KNOWLEDGE REQUIRED BY THE POSITION

- Knowledge of information security principles, methods and best practices.
- Knowledge of security threats and IT risk management principles.
- Knowledge of disaster planning and recovery principles.
- Knowledge of firewalls, intrusion detection/prevention, SIEM systems, and endpoint protection platforms.
- Knowledge of network hardware, protocols, and standards.
- Knowledge of county business processes.
- Skill in communicating complex ideas both orally and in writing and ability to convey technical concepts to non-technical staff.
- Skill in analyzing network traffic, logs and system behavior to identify anomalies.
- Skill in troubleshooting and resolving IT system issues.
- Skill in preparing clear and concise reports from multiple data sources.
- Skill in establishing and maintaining effective working relationships.

SUPERVISORY CONTROLS

The Information Technology Director assigns work in terms of very general instructions. The supervisor spot-checks completed work for compliance with procedures and the nature and propriety of the final results.

GUIDELINES

Guidelines include CJIS, DHS and FBI requirements for data access and handling; county and department Policies and procedures. These guidelines require judgement, selection and interpretation in application.

COMPLEXITY/SCOPE OF WORK

- The work consists of varied IT systems administration duties. The broad range of assets and digital infrastructure combined with the changing threat environment contribute to the complexity of the position.
- The purpose of this position is to safeguard the County's information assets and digital infrastructure. Successful performance contributes to the efficiency and effectiveness of a variety of county operations.

CONTACTS

- Contacts are typically with co-workers, other county employees, vendors, members of the general public.
- Contacts are typically to give or exchange information, resolve problems, and provide services.

PHYSICAL DEMANDS/ WORK ENVIRONMENT

- The work is typically performed while sitting at a desk or table or while intermittently sitting, standing, or stooping. The employee occasionally lifts heavy (25 pounds or more) objects, uses tools or equipment requiring a high degree of dexterity, and distinguishes between shades of color.
- The work is typically performed in an office or computer room.

SUPERVISORY AND MANAGEMENT RESPONSIBILITY

None.

MINIMUM QUALIFICATIONS

- Knowledge and level of competency commonly associated with the completion of a baccalaureate degree in Cybersecurity, Computer Science, Information Technology, or related field.
- Sufficient experience to understand the basic principles relevant to the major duties of the position, usually associated with the completion of an apprenticeship/internship or having had a similar position for at least three years.
- Possession of **Security+**, **CySA+**, or **equivalent certification** required upon hire or within six (6) months.
- **CISSP**, **CISM**, **CEH**, or equivalent advanced certification preferred.
- Must obtain **NCIC certification** within six (6) months of employment.
- Possession of or ability to readily obtain a valid driver's license issued by the State of Iowa for the type of vehicle or equipment operated.