DATE: APRIL 2024
FLSA: NON-EXEMPT
SALARY: GRADE T
CBA DESIGNATION: CLASSIFIED BARGAINING UNIT

CYBERSECURITY ANALYST

BASIC FUNCTION

Implements and administers cybersecurity measures to ensure the protection of the District's network infrastructure, systems, and resources; advises on network designs, security configurations, device standards and compliance, and network access policies to identify and remediate vulnerabilities, protect against threats, and assess and mitigate risk; deploys and maintains cybersecurity systems, including firewalls, intrusion prevention systems, and email security solutions.

SUPERVISION RECEIVED AND EXERCISED

Receives general supervision from assigned area supervisor. May provide lead direction to temporary staff and/or student workers.

CLASS CHARACTERISTICS

This classification is responsible for independently performing professional support to the District's cybersecurity needs. Incumbents regularly work on tasks which are varied and complex, requiring considerable discretion and independent judgment. Employees in the classification rely on experience and judgment to perform assigned duties and ensure the security and integrity of District resources. Assignments are given with general guidelines. Work is typically reviewed upon completion for soundness, appropriateness, and conformity to policy and requirements

EXAMPLES OF TYPICAL JOB FUNCTIONS

1. Serves a key role for the architecture, planning, and implementation of the District's network and telecommunication infrastructure.
2. Recommends, implements, installs, and maintains systems for: monitoring cybersecurity risks, vulnerabilities, threats, and breaches; enterprise-level account and email security; account lifecycles, mailboxes, listservs, and other collaboration services; remote access policies and services; and data management, classification, lifecycles, and loss prevention.
3. Researches and collaborates with consultants in continual assessments to identify recommendations to improve cybersecurity systems for the District.
4. Continually reviews emerging industry threats and provides direction when and where necessary.
5. Provides risk assessment and mitigation solutions for identified risks and vulnerabilities.
6. Responds, reports, and coordinates incident response to threats and breaches.
7. Advises on protection strategies for all organizational assets that are susceptible to digital and physical threats.
8. Reviews new software and technology solutions for security standards and compliance.
9. Assists the District in updating policies, standards, procedures, and practices to increase the District's cybersecurity, as well as maintain legislative and regulatory compliance, e.g., FERPA, HIPAA, PCI, and GLBA.
10. Develops and coordinates cybersecurity awareness trainings to foster a cybersecurity-first culture.
11. Maintains records, diagrams, and processes relating to areas of administration.
12. Compiles data for investigations for, but not limited to, public records requests and subpoenas.
13. Participates in District-provided in-service training programs.
14. Performs other related duties as assigned; specific duties not listed does not exclude them for this classification if the work is similar or related.

QUALIFICATIONS

Knowledge of:

1. Operations, services, and activities of a comprehensive cybersecurity program.
2. Network perimeter/edge design and management principles and techniques.
3. Operational characteristics of network and telecommunication systems hardware, software, and peripheral equipment and devices.
4. Industry best practices in cybersecurity measures for enterprise network systems, infrastructure, and services.
5. Methods and techniques of evaluating cybersecurity threats and responding accordingly.
6. Server-based operating systems and software, including system standards and protocols.
7. Diagnostic tools and utilities used in threat detection and response.
8. Interconnections and relationships across multiple technology services and operations.
9. Technology threat/intrusion protection systems and devices.

Ability to:

1. Perform a variety of specialized security related duties in support of the District's network and telecommunication systems.
2. Develop, design, and implement enterprise level network/edge and related security measures.
3. Monitor security measure effectiveness and recommend changes to optimize system resistance to security threats and breaches.
4. Implement solutions to monitor and ensure the integrity of systems and data.
5. Troubleshoot, detect, and resolve security related issues.
6. Utilize diagnostic and testing tools to detect and resolve security breaches.
7. Prepare clear, concise, and accurate reports and technical documentation.
8. Research and maintain knowledge of best management practices for cybersecurity programs, diagnostic tools, and mitigation measures.
9. Independently organize work, set priorities, meet critical deadlines, and follow up on assignments.
10. Use tact, initiative, prudence, and independent judgment within general policy and procedural guidelines.
11. Maintains current knowledge of cybersecurity technologies, standards, and best practices.
12. Effectively use computer systems, software applications relevant to work performed, and business equipment to perform a variety of work tasks.
13. Communicate effectively in the course of performing work tasks.
14. Establish, maintain, and foster effective working relationships with those contacted in the course of work.
15. Demonstrate clear evidence of sensitivity and understanding of the diverse academic, socio-economic, disability, and ethnic backgrounds of students, staff, and the community.
16. Provide efficient, high-level customer service to the public, vendors, contractors, and District personnel.

Education and Experience:

An associate's degree in computer science or a closely related field and four (4) years of networking and cybersecurity experience; or an equivalent combination of education, training, and/or experience.

Licenses and Certifications:

A valid driver's license and proof of insurability may be required to drive a District or personal vehicle.

PHYSICAL DEMANDS

Must possess mobility to work in indoor and outdoor areas where networking equipment exists and in a standard office setting and use standard office equipment, including a computer; vision to read printed materials and a computer screen; and hearing and speech to communicate in person and over the telephone. Finger dexterity is needed to access, enter, and retrieve data using a computer keyboard or calculator and to operate standard office equipment. Employees in this classification occasionally bend, stoop, kneel, reach, use a step ladder, push, and pull drawers open and closed to retrieve and file information. Employees must possess the ability to lift, carry, push, and pull materials and objects up to 50 pounds.

The essential functions of this classification must be performed by the incumbents with or without reasonable accommodations.

ENVIRONMENTAL CONDITIONS

Employees work in an office environment with moderate noise levels, controlled temperature conditions, and no direct exposure to hazardous physical substances. Employees will also work in indoor and outdoor areas where networking equipment exists with various noise levels, ambient temperature, and environmental conditions. Employees may interact with upset individuals in interpreting and enforcing departmental policies and procedures.