JOB TITLE:	ADMINISTRATOR CYBERSECURITY
DIVISION	TECHNOLOGY
SALARY SCHEDULE/GRADE:	II, GRADE 7
WORK YEAR:	AS APPROVED BY THE BOARD
FLSA STATUS:	EXEMPT
JOB CLASS CODE:	8524
BARGAINING UNIT:	CLAS

REVISED: 07/20/2022

Submitted: 07/19/2022

SCOPE OF RESPONSIBILITIES
Coordinates information security initiatives with vendors and auditors district-wide. Monitors information security risks and enhances the district's cybersecurity posture by implementing, testing, and managing information security best practices. Responds to cyber incidents and operationalizes policies and procedures to protect the District against cyber threats.

PERFORMANCE RESPONSIBILITIES & EVALUATION CRITERIA
Manages users and groups in Active Directory and assigns approved resources and network privileges; manages and administers email mailboxes, distribution lists, and related resources
Equips and manages all aspects of systems security and ensures auditing requirements are met for all security access; works with internal stakeholders and coordinates with outside vendors/agencies during information/cybersecurity assessments, audits, and exercises
Creates, records, verifies, audits, and maintains the changes effected to privileged access across the technology infrastructure, and engages with other staff in promoting and sustaining effective enterprise change management practices
Manages security and compliance solutions like Data Loss Prevention (DLP) and performs hand on vulnerability and penetration tests to identify and defend against threats
Performs risk analysis and implements recommendations for application security, access control, and enterprise data safeguards to defend systems against unauthorized access, modification or destruction
Identifies opportunities to reduce information security risks and promptly documents and communicates mitigation options to team members and management
Conducts data and system security tests to ensure compliance with applicable laws, Service Legal Agreements (SLAs), and policies; enhances the District's overall cybersecurity posture by designing, implementing, testing, and maintaining verifiable and repeatable industry-standard practices to ensure the integrity, availability, and confidentiality of sensitive data and reports on findings and recommendations for corrective action
Operationalizes policies and procedures related to the chosen cybersecurity framework and ensures compliance; consults with staff, manager, and executives about the best security practices and provides technical advice
Monitors system, access, and security logs and reviews threat analytics including defining and running daily health checks on applicable technology and infrastructure systems as required; responds to system alerts and security incidents in a primary contact role during or after business hours, while engaging with other team members and stakeholders within and outside of the organization, to mitigate cyber-security risks
Stays abreast of emerging threats and vulnerabilities and designs, communicates, and implements best practices to secure information and to enhance the availability and integrity of information and infrastructure systems; assesses, tests, and recommends new security products and technologies where necessary
Evaluates staff as assigned
Performs other duties as assigned by supervisor
Completes all trainings and other compliance requirements as assigned by the designated deadline

PHYSICAL DEMANDS

The work is primarily sedentary. The work requires the use of hands for simple grasping and fine manipulations. The work at times requires bending, squatting, crawling, climbing and reaching, with the ability to lift, carry, push or pull moderate weights.

MINIMUM QUALIFICATIONS
Bachelor's degree in computer science or cybersecurity field
One (1) year of verifiable experience in Information Security and a strong understanding of cybersecurity frameworks.
A current, relevant, and industry-recognized certification or ability to successfully complete department-designated and department-paid certification(s) within twelve (12) months of hire
Effective communication skills

DESIRABLE QUALIFICATIONS
Analytical, conceptual, and problem-solving abilities
Ethical hacking and penetration testing/vulnerability assessment experience
Experience in a diverse workplace