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

NEW: 07/20/2022

Submitted: 07/19/2022

SCOPE OF RESPONSIBILITIES

Plans, coordinates, deploys, and monitors enterprise hardware and campus-wide systems. Manages O365/Azure Active Directory users and groups, email mailboxes, distribution lists, and resources. Supports project tasks including monitoring system performance, receiving, analyzing, and tracking customer trouble tickets, defining/coordinating solutions, testing hardware and software solutions

PERFORMANCE RESPONSIBILITIES & EVALUATION CRITERIA

- Manages the O365/Azure Active Directory implementation and assigns approved resources and network privileges; manages and administers email mailboxes, distribution lists, and related resources
- Diagnoses and troubleshoots enterprise hardware and campus-wide application deployments and provides satisfactory resolution in a timely fashion
- Monitors premise and cloud-hosted systems, including defining and running daily health checks proactively and responds to system alerts in a primary contact role while engaging other team members to troubleshoot and resolve system issues
- Tests enterprise hardware and system changes before deployment to ensure security best practices; promptly documents and disseminates findings to the team members and collaborates with team members to satisfactorily resolve issues discovered during the tests
- Resolves relevant trouble tickets to the satisfaction of the initiator in a timely fashion and ensures the tickets complete their lifecycle
- Executes multiple concurrent projects and utilizes effective time management, planning, and people skills to liaise with other team members and customers to ensure timely delivery of projects and to provide a timely status update to all project stakeholders
- Creates and maintains system documentation, diagrams, and coordinates with vendors and other business units to ensure the viability of the infrastructure
- Performs enterprise hardware and software upgrades, maintains system configurations, and deploys campus-wide patches and software packages
- Stays current on vendor certification(s) by completing updated certification exams by the specified deadline and keeps related hardware and software skills updated
- Participates in projects, upgrades, outages and is available to assist after hours as needed by the team
- Performs other duties as assigned by supervisor
- Completes all training and other compliance requirements by the designated deadline

PHYSICAL DEMANDS

The work is primarily sedentary. The work at times requires bending, squatting, crawling, climbing, reaching with the ability to lift, carry, push, or pull light weights. The work requires the use of hands for simple grasping and fine manipulations. The work requires activities involving being around moving machinery, driving automotive equipment, exposure to marked

changes in temperature and humidity and exposure to dust, fumes, and gases. The work requires the use of feet for repetitive movements.

MINIMUM QUALIFICATIONS
Bachelor’s degree
Experience managing or supporting the hardware and systems infrastructure, preferably in a mid-large enterprise setting
A current, relevant, and industry-recognized certification or ability to complete department-designated and department-paid certification(s) within twelve (12) months of hire
Effective communication skills

DESIRABLE QUALIFICATIONS
Strong understanding of Azure/O365 Active Directory, Office 365, and virtualization technologies
Experience in SCCM/Intune or other software deployment tools
Experience managing thin client solutions in an enterprise setting
Project management experience
Experience in a diverse workplace

JOB TITLE:	COORDINATOR SYSTEMS INTEGRATION
DIVISION	TECHNOLOGY
SALARY SCHEDULE/GRADE:	II, GRADE 7
WORK YEAR:	260 DAYS
FLSA STATUS:	EXEMPT
JOB CLASS CODE:	
BARGAINING UNIT:	CLAP

NEW: 07/20/2022

Submitted: 07/19/2022

SCOPE OF RESPONSIBILITIES

Provides all teachers and District personnel seamless and secure access to an online asset and service management system. Assists with the implementation of Districtwide technology projects and all aspects of technology integration.

PERFORMANCE RESPONSIBILITIES & EVALUATION CRITERIA

- Works cooperatively with IT3 stakeholders in assessing and addressing the district's technology priorities and needs in order to develop, review and revise programs or activities
- Serves as liaison between schools, vendors and internal stakeholders by facilitating, documenting and automating various concurrent integration processes and workflows; including but not limited to, the asset and service management system
- Supervises and directs the work of individuals, committees, and task forces, as assigned
- Monitors concurrent project plans to ensure projects are completed according to schedule
- Verifies the accuracy and completeness of work performed by assigned staff and effectively communicates ideas of improvement to team members in a proactive manner
- Organizes and implements technology related projects to ensure the efficient use of district resources as well as the secure operation of information systems.
- Provides virtual support to end users to ensure effective integration of the asset and service management system
- Provides technical recommendations based on needs analyses of project requirements, business operations, employment practices, instructional practices and technical skills
- Ensures compliance with local, state and federal regulations and procedures related to area of assignment
- Performs other duties as assigned by supervisor
- Completes all trainings and other compliance requirements as assigned and by the designated deadline

PHYSICAL DEMANDS

The work is primarily sedentary. The work at times requires bending, squatting, crawling, climbing, reaching with the ability to lift, carry, push, or pull light weights. The work requires the use of hands for simple grasping and fine manipulations. The work requires activities involving being around moving machinery, driving automotive equipment, exposure to marked changes in temperature and humidity and exposure to dust, fumes, and gases. The work requires the use of feet for repetitive movements. The work requires activities involving driving automotive equipment.

MINIMUM QUALIFICATIONS

- High school diploma or G.E.D.
- Three (3) years of technical training/experience
- Three (3) years of experience in computer operations
- Valid Driver’s License

Understanding of networking architecture and state statutes regarding student information privacy and security

DESIRABLE QUALIFICATIONS
Associates degree, or above in Computer Science
Experience in documenting/ensuring student information privacy and security
Experience in a diverse workplace

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

~~NEW:~~ Revised: Submitted:

07/20/2022 07/19/2022

~~07/01/2019~~ ~~06/11/2019~~

SCOPE OF RESPONSIBILITIES

~~Plans, coordinates, and monitors systems hardware and application software. Equips and manages Active Directory users and groups as well as email mailboxes, distribution lists and resources.~~ ~~Coordinates information~~ ~~security initiatives with vendors and auditors.~~ 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

~~Equips and m~~ 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
~~Tests data center hardware and software changes prior to deployment to ensure security best practices; promptly documents and disseminates findings to the team members and subsequently collaborates with team members to satisfactorily resolve issues discovered during the tests~~
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 ~~related~~ cybersecurity field
~~Two (2) years~~ One (1) year of ~~demonstrable and~~ verifiable experience in Information Security and a strong understanding of cybersecurity frameworks. ~~supporting the hardware and systems infrastructure focused on information security~~
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

~~Strong understanding of NIST, ISO cybersecurity frameworks~~
Analytical, conceptual, and problem-solving abilities
Ethical hacking and penetration testing/vulnerability assessment experience
Experience in a diverse workplace

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