JOB TITLE:	COORDINATOR NETWORK
DIVISION	TECHNOLOGY
SALARY SCHEDULE/GRADE:	II/GRADE 7
WORK YEAR:	AS APPROVED BY THE BOARD
FLSA STATUS:	EXEMPT
JOB CLASS CODE:	8569
BARGAINING UNIT:	CLAP

REVISED: ~~08/30/2023~~ 03/27/2024

Submitted: ~~08/29/2023~~ 03/26/2024

SCOPE OF RESPONSIBILITIES
Maintains the computing environment by identifying network requirements, installing upgrades/updates, and monitors network and IPT performance. Provides daily technical support for identifying, troubleshooting and resolving data and voice network issues. Works closely with the network and infrastructure services teams to ensure network uptime and ensures all network equipment are updated/upgraded and backed up as per industry-standard best practices. Assists network engineer and other team members in identifying and mitigating risks and vulnerabilities.

PERFORMANCE RESPONSIBILITIES & EVALUATION CRITERIA
Establishes LAN/WAN network specifications according to established policies and procedures by analyzing workflow, access, information, and security requirements
Maintains network performance by performing network monitoring, analysis, and performance tuning; troubleshoots and resolves network problems utilizing appropriate analytical tools and test equipment; escalates problems to vendor; follows ITIL standards and established SLAs to conduct root-cause analysis of events and coordinates with vendor tickets to ensure complete issue resolution
Administers and configures routers and related equipment including interface configuration and routing protocols
Secures the network by developing network access, monitoring, control, and evaluation, and is available on call 24 hours a day, seven days a week
Assists the network engineer in the creation and maintenance of the network documentation and follows enterprise change control methodologies to affect necessary changes to the network infrastructure
Upgrades the network by conferring with vendors and team members; develops, tests, evaluates, installs enhancements, and communicates effectively and promptly with the team, internal and external customers and vendors
Protects the organization's value by keeping information confidential and assists end-users in data/network security related matters
Accomplishes organization goals by accepting ownership for accomplishing new and different requests and explores opportunities to add value to job accomplishments
Keeps abreast of emerging trends and threats and implements appropriate mitigation measures; stays current on certifications by successfully completing updated certification exams
Evaluated staff as assigned
Completes all trainings and other compliance requirements as assigned and by the designated deadline
Regular, predictable performance is required for all performance responsibilities
This position requires collaboration, customer support, and team interaction.

Performs other duties as assigned by supervisor

PHYSICAL DEMANDS
~~The work requires the use of hands for simple grasping and fine manipulations. The work at times requires bending, squatting, crawling, climbing, reaching, with the ability to lift, carry, push or pull light weights.~~ This position requires the following physical activities rarely (up to 25% of the workweek): balancing, bending, climbing, crawling, crouching, driving, kneeling, and reaching. The following physical activities are required occasionally (up to 50% of the workweek): lifting up to 20 lbs., pulling up to 20 lbs., pushing up to 20 lbs., standing, and walking. Feeling, grasping, hearing, and talking are required frequently (up to 75% of the workweek). Repetitive motions and visual acuity are required constantly (up to 100% of the workweek).

MINIMUM QUALIFICATIONS
Associate's degree or one (1) year demonstrable experience supporting infrastructure, preferably in a mid to large organization
~~One (1) year of demonstrable experience supporting network infrastructure, preferably in a mid to large organization~~
Excellent written and oral communication skills coupled with thorough knowledge of enterprise networking methodologies and protocols including configuring and managing enterprise network equipment.
A current, relevant, and industry-recognized certification or ability to complete department-designated and department- paid certification(s) within twelve (12) months of hire

DESIRABLE QUALIFICATIONS
Bachelor's degree
Experience leading a team of network support staff.
Experience in enterprise LAN/WAN design and network security
Experience in a diverse workplace

JOB TITLE:	COORDINATOR NETWORK
DIVISION	TECHNOLOGY
SALARY SCHEDULE/GRADE:	II/GRADE 7
WORK YEAR:	AS APPROVED BY THE BOARD
FLSA STATUS:	EXEMPT
JOB CLASS CODE:	8569
BARGAINING UNIT:	CLAP

REVISED: 03/27/2024

Submitted: 03/26/2024

SCOPE OF RESPONSIBILITIES
Maintains the computing environment by identifying network requirements, installing upgrades/updates, and monitors network and IPT performance. Provides daily technical support for identifying, troubleshooting and resolving data and voice network issues. Works closely with the network and infrastructure services teams to ensure network uptime and ensures all network equipment are updated/upgraded and backed up as per industry-standard best practices. Assists network engineer and other team members in identifying and mitigating risks and vulnerabilities.

PERFORMANCE RESPONSIBILITIES & EVALUATION CRITERIA
Establishes LAN/WAN network specifications according to established policies and procedures by analyzing workflow, access, information, and security requirements
Maintains network performance by performing network monitoring, analysis, and performance tuning; troubleshoots and resolves network problems utilizing appropriate analytical tools and test equipment; escalates problems to vendor; follows ITIL standards and established SLAs to conduct root-cause analysis of events and coordinates with vendor tickets to ensure complete issue resolution
Administers and configures routers and related equipment including interface configuration and routing protocols
Secures the network by developing network access, monitoring, control, and evaluation, and is available on call 24 hours a day, seven days a week
Assists the network engineer in the creation and maintenance of the network documentation and follows enterprise change control methodologies to affect necessary changes to the network infrastructure
Upgrades the network by conferring with vendors and team members; develops, tests, evaluates, installs enhancements, and communicates effectively and promptly with the team, internal and external customers and vendors
Protects the organization's value by keeping information confidential and assists end-users in data/network security related matters
Accomplishes organization goals by accepting ownership for accomplishing new and different requests and explores opportunities to add value to job accomplishments
Keeps abreast of emerging trends and threats and implements appropriate mitigation measures; stays current on certifications by successfully completing updated certification exams
Evaluated staff as assigned
Completes all trainings and other compliance requirements as assigned and by the designated deadline
Regular, predictable performance is required for all performance responsibilities
This position requires collaboration, customer support, and team interaction.
Performs other duties as assigned by supervisor

PHYSICAL DEMANDS
This position requires the following physical activities rarely (up to 25% of the workweek): balancing, bending, climbing, crawling, crouching, driving, kneeling, and reaching. The following physical activities are required occasionally (up to 50% of the workweek): lifting up to 20 lbs., pulling up to 20 lbs., pushing up to 20 lbs., standing, and walking. Feeling, grasping, hearing, and talking are required frequently (up to 75% of the workweek). Repetitive motions and visual acuity are required constantly (up to 100% of the workweek).

MINIMUM QUALIFICATIONS
Associate's degree or one (1) year demonstrable experience supporting infrastructure, preferably in a mid to large organization
Excellent written and oral communication skills coupled with thorough knowledge of enterprise networking methodologies and protocols including configuring and managing enterprise network equipment.
A current, relevant, and industry-recognized certification or ability to complete department-designated and department- paid certification(s) within twelve (12) months of hire

DESIRABLE QUALIFICATIONS
Bachelor's degree
Experience leading a team of network support staff.
Experience in enterprise LAN/WAN design and network security
Experience in a diverse workplace

JOB TITLE:	COORDINATOR ~~INFORMATION SECURITY~~ SYSTEMS ADMINISTRATOR
DIVISION	TECHNOLOGY
SALARY SCHEDULE/GRADE:	II/GRADE 7
WORK YEAR:	260 DAYS
FLSA STATUS:	EXEMPT
JOB CLASS CODE:	8571
BARGAINING UNIT:	CLAP

REVISED:
~~07/01/0219~~
7/01/2024

Submitted:
~~06/11/2019~~
03/26/2024

SCOPE OF RESPONSIBILITIES

~~Configures, administers, and supports systems, and services of the technology infrastructure. Proactively monitors logs, and usage analytics to identify and mitigate threat vectors across all systems to ensure high availability and security of information and information systems. Communicates across various teams and all stakeholders and supports critical technology projects.~~

Plans, coordinates, deploys, administers, and monitors enterprise technology services and district-wide systems. Supports critical services such as Microsoft 365/Azure Active Directory with a focus on users and groups, group policies, conditional access controls, 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

~~Designs, configures, monitors, maintains, documents, and supports all aspects of the technology infrastructure including related systems, hardware, software, services, configurations, documentation, and policies; technology infrastructure includes (but not limited to): network systems and software, virtual and physical servers, desktop environment, Windows Active Directory/Group Policy Objects (GPO), Office 365, voice over IP (VOIP) telecommunications system and all connected devices, and print services management tools~~

Works with other assigned administrators to manage the district's Microsoft 365/Azure Active Directory implementation and assigns approved resources and network privileges; manages and administers email mailboxes, distribution lists, and related resources

~~Monitors switches, servers, routers, firewalls, wireless components, backups, network segmentation routes, and other physical or virtual environments including virtual appliances using enterprise and vendor-specific monitoring tools; creates and manages proactive monitoring and alerting environments with automated alert notifications and ticketing to ensure high availability and security of all systems~~

Diagnoses and troubleshoots enterprise technology services and district-wide application deployments and provides satisfactory resolution in a timely fashion

~~Monitors and analyzes system logs, usage analytics, and anti-virus logs to identify threat vectors and performs required notification and remediation actions to minimize/eliminate the threats, and follows established Service Level Agreements and associated protocols~~

Collaborates with colleagues to evaluate, engineer, and support solutions for device management at a district level as needed

~~Develops and constantly maintains infrastructure-related technical documentation including diagrams, schematics, templates, configuration documents, and all other materials~~

Monitors on-premise, cloud-hosted, and SaaS 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; responds to critical issues as they occur during or outside of regular business hours

~~Monitors network and other vital systems and responds to the system, hardware, and software failures and outages promptly; responds to critical issues as they occur during or outside of regular business hours~~

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

~~Collaborates and communicates effectively and courteously with Information Technology team members as well as other internal and external stakeholders to provide technical support and assistance to staff members, as needed; acts as a Tier 3/4/Level responder to help desk requests and related support needs~~

Supports efforts to proactively monitor logs and usage analytics to identify and mitigate threat vectors across all systems to ensure high availability and information integrity; coordinates with the cyber team and assists in information security forensics and remediations as needed

~~Promotes Continuous Quality Improvement (CQI) by proactively identifying and helping to identify and implement improvements and best practices, and promotes a culture of innovation by identifying and developing ideas and innovative methods to enhance operational efficiency and improving technical capability~~
Assumes oversight responsibility for a specific district-wide hardware or software solution, if assigned by their supervisor
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 district-wide patches and software packages
Participates in projects, upgrades, outages and is available to assist after hours as needed by the team
Stays current on the latest technology and network trends, concepts, and threats, and constantly finds a way to strengthen and improve the network and technology infrastructure
Stays current on vendor certification(s) by completing updated certification exams by the specified deadline and keeps related hardware and software skills updated
Performs other duties as assigned by supervisor
Completes all trainings and other compliance requirements as assigned and by the designated deadline
Regular, predictable performance is required for all performance responsibilities
This position requires collaboration, customer support, and team interaction

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.~~This position requires the following physical activities rarely (up to 25% of the workweek): balancing, bending, climbing, crawling, crouching, driving, kneeling, and reaching. The following physical activities are required occasionally (up to 50% of the workweek): lifting up to 50 lbs., pulling up to 50 lbs., pushing up to 50 lbs., standing, and walking. Feeling, grasping, hearing, and talking are required frequently (up to 75% of the workweek). Repetitive motions and visual acuity are required constantly (up to 100% of the workweek).
MINIMUM QUALIFICATIONS
Associate's degree in computer science or related field or (1) one year of verifiable experience supporting an enterprise hardware or software systems infrastructure.
~~Three (3) years of verifiable experience supporting an enterprise hardware an software systems infrastructure~~
A current, relevant, and industry-recognized certification, or the ability to complete department designated and department-paid certification(s) within twelve (12) months of hire.
~~In-depth knowledge of network and security protocols~~
~~Project management and network monitoring experience~~
Effective communication skills
DESIRABLE QUALIFICATIONS
Bachelor's Degree in Computer Science or related field
PMP, ITIL, CompTIA A+, Net+, Security +, MCSE and other Microsoft Certifications
Strong understanding of Azure/Microsoft 365 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

REVISED: 07/01/2024

SUBMITTED: 03/26/2024

JOB TITLE:	COORDINATOR SYSTEMS ADMINISTRATOR
DIVISION	TECHNOLOGY
SALARY SCHEDULE/GRADE:	II/GRADE 7
WORK YEAR:	260 DAYS
FLSA STATUS:	EXEMPT
JOB CLASS CODE:	8571
BARGAINING UNIT:	CLAP

SCOPE OF RESPONSIBILITIES
Plans, coordinates, deploys, administers, and monitors enterprise technology services and district-wide systems. Supports critical services such as Microsoft 365/Azure Active Directory with a focus on users and groups, group policies, conditional access controls, 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
Works with other assigned administrators to manage the district's Microsoft 365/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 technology services and district-wide application deployments and provides satisfactory resolution in a timely fashion
Collaborates with colleagues to evaluate, engineer, and support solutions for device management at a district level as needed
Monitors on-premise, cloud-hosted, and SaaS 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; responds to critical issues as they occur during or outside of regular business hours
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
Supports efforts to proactively monitor logs and usage analytics to identify and mitigate threat vectors across all systems to ensure high availability and information integrity; coordinates with the cyber team and assists in information security forensics and remediations as needed
Assumes oversight responsibility for a specific district-wide hardware or software solution, if assigned by their supervisor
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 district-wide patches and software packages
Participates in projects, upgrades, outages and is available to assist after hours as needed by the team
Stays current on the latest technology and network trends, concepts, and threats, and constantly finds a way to strengthen and improve the network and technology infrastructure
Stays current on vendor certification(s) by completing updated certification exams by the specified deadline and keeps related hardware and software skills updated
Performs other duties as assigned by supervisor
Completes all trainings and other compliance requirements as assigned and by the designated deadline
Regular, predictable performance is required for all performance responsibilities
This position requires collaboration, customer support, and team interaction

PHYSICAL DEMANDS
This position requires the following physical activities rarely (up to 25% of the workweek): balancing, bending, climbing, crawling, crouching, driving, kneeling, and reaching. The following physical activities are required occasionally (up to 50% of the workweek): lifting up to 50 lbs., pulling up to 50 lbs., pushing up to 50 lbs., standing, and walking. Feeling, grasping, hearing, and talking are required frequently (up to 75% of the workweek). Repetitive motions and visual acuity are required constantly (up to 100% of the workweek).
MINIMUM QUALIFICATIONS
Associate's degree in computer science or related field or (1) one year of verifiable experience supporting an enterprise hardware or software systems infrastructure.
A current, relevant, and industry-recognized certification, or the ability to complete department designated and department-paid certification(s) within twelve (12) months of hire.
Effective communication skills
DESIRABLE QUALIFICATIONS
Bachelor's Degree in Computer Science or related field
PMP, ITIL, CompTIA A+, Net+, Security +, MCSE and other Microsoft Certifications
Strong understanding of Azure/Microsoft 365 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~~ PLATFORM ADMINISTRATION
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~~: Revised: ~~07/20/2022~~ 07/01/2024

Submitted: ~~07/19/2022~~ 03/26/2024

SCOPE OF RESPONSIBILITIES

Plans, coordinates, deploys, administers, and monitors enterprise ~~hardware~~ technology services and ~~campus~~ district-wide systems. ~~Manages~~ Administers key enterprise platforms such as ~~O~~Microsoft 365/Azure Active Directory with a focus on users and groups, group policies, conditional access controls, 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

Works with other assigned administrators to ~~M~~manage the district's Microsoft ~~O~~365/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~~ technology services and ~~campus~~ district-wide application deployments and provides satisfactory resolution in a timely fashion

Collaborates with colleagues to evaluate, engineer, and support solutions for device management at a district level as needed

Monitors on-premise ~~and,~~ cloud-hosted, and SaaS 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; responds to critical issues as they occur during or outside of regular business hours

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

Supports efforts to proactively monitor logs and usage analytics to identify and mitigate threat vectors across all systems to ensure high availability and information integrity; coordinates with the cyber team and assists in information security forensics and remediations as needed

If assigned by their supervisor, assumes oversight responsibility for a specific district-wide hardware or software solution

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 district-wide patches and software packages

Stays current on the latest technology trends, concepts, and threats, and constantly finds ways to strengthen and improve the technology infrastructure
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
Regular, predictable performance is required for all performance responsibilities
This position requires collaboration, customer support, and team interaction

PHYSICAL DEMANDS
~~The work is primarily sedentary. The work at times requires bending, squatting, crawling, climbing, reaching with he ability to life, carry, push, or pull light weights.~~ This work is conducted in an office setting. This position has inside environmental conditions with protection from weather conditions but not necessarily from temperature changes or atmospheric conditions while working on performance responsibilities. This position requires the following physical activities rarely (up to 25% of the workweek): balancing, bending, climbing, crawling, crouching, driving, kneeling, and reaching. The following physical activities are required occasionally (up to 50% of the workweek): lifting up to 50 lbs., pulling up to 50 lbs., pushing up to 50 lbs., standing, and walking. Feeling, grasping, hearing, and talking are required frequently (up to 75% of the workweek). Repetitive motions and visual acuity are required constantly (up to 100% of the workweek).

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/Microsoft ~~O~~365 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 PLATFORM ADMINISTRATION
DIVISION	TECHNOLOGY
SALARY SCHEDULE/GRADE:	II/GRADE 7
WORK YEAR:	AS APPROVED BY THE BOARD
FLSA STATUS:	EXEMPT
JOB CLASS CODE:	
BARGAINING UNIT:	CLAS

Revised: 07/01/2024

Submitted: 03/26/2024

SCOPE OF RESPONSIBILITIES

Plans, coordinates, deploys, administers, and monitors enterprise technology services and district-wide systems. Administers key enterprise platforms such as Microsoft 365/Azure Active Directory with a focus on users and groups, group policies, conditional access controls, 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

Works with other assigned administrators to manage the district's Microsoft 365/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 technology services and district-wide application deployments and provides satisfactory resolution in a timely fashion

Collaborates with colleagues to evaluate, engineer, and support solutions for device management at a district level as needed

Monitors on-premise, cloud-hosted, and SaaS 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; responds to critical issues as they occur during or outside of regular business hours

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

Supports efforts to proactively monitor logs and usage analytics to identify and mitigate threat vectors across all systems to ensure high availability and information integrity; coordinates with the cyber team and assists in information security forensics and remediations as needed

If assigned by their supervisor, assumes oversight responsibility for a specific district-wide hardware or software solution

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 district-wide patches and software packages

Stays current on the latest technology trends, concepts, and threats, and constantly finds ways to strengthen and improve the technology infrastructure
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
Regular, predictable performance is required for all performance responsibilities
This position requires collaboration, customer support, and team interaction

PHYSICAL DEMANDS

This work is conducted in an office setting. This position has inside environmental conditions with protection from weather conditions but not necessarily from temperature changes or atmospheric conditions while working on performance responsibilities.

This position requires the following physical activities rarely (up to 25% of the workweek): balancing, bending, climbing, crawling, crouching, driving, kneeling, and reaching. The following physical activities are required occasionally (up to 50% of the workweek): lifting up to 50 lbs., pulling up to 50 lbs., pushing up to 50 lbs., standing, and walking. Feeling, grasping, hearing, and talking are required frequently (up to 75% of the workweek). Repetitive motions and visual acuity are required constantly (up to 100% of the workweek).

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/Microsoft 365 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

REVISED: Submitted:
~~07/01/2019~~ ~~06/11/2019~~
07/01/2024 03/26/2024

JOB TITLE:	~~ADMINISTRATOR~~ COORDINATOR CYBERSECURITY ADMINISTRATION
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

SCOPE OF RESPONSIBILITIES
~~Plans,~~ C~~c~~oordinates, ~~and monitors systems hardware and application software. Equips and manages Active directory users and groups as well as email mailboxes, distribution lists and resources.~~ information security initiatives with internal stakeholders, vendors and auditors, for the purpose of protecting JCPS information systems and data. Monitors information security risks and enhances the district's cybersecurity posture by researching, recommending, implementing, testing, and managing information security best practices. Work both independently and with team members within the established procedures to protect against unauthorized system access, information modifications, and data destruction.

PERFORMANCE RESPONSIBILITIES & EVALUATION CRITERIA
~~Equips and manages users and~~ groups in ~~Active directory and assigns approved resources and network privileges; manages and administers email mailboxes, distribution lists, and related resources.~~ Serves as a member of the JCPS Cyber Security Operations Center (CSOC) which focuses on providing situational threat awareness and management of the district's security posture; the limited size of the JCPS cyber team will require that the CSOC collaborate effectively with other IT colleagues as well as external vendors as needed.
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.~~ Collaborates with other IT colleagues to review and test 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
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, 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
Routinely m~~M~~onitors 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

Participates in projects, upgrades, outages and is available to assist after hours as needed by the team
~~Evaluates staff as assigned~~
Performs other duties as assigned by supervisor
Completes all trainings and other compliance requirements as assigned by the designated deadline
Regular, predictable performance is required for all performance responsibilities
This position requires collaboration, customer support, and team interaction

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.~~ This work is conducted in an office setting. This position has inside environmental conditions with protection from weather conditions but not necessarily from temperature changes or atmospheric conditions while working on performance responsibilities.

This position requires the following physical activities rarely (up to 25% of the workweek): balancing, bending, climbing, crawling, crouching, driving, kneeling, and reaching. The following physical activities are required occasionally (up to 50% of the workweek): lifting up to 50 lbs., pulling up to 50 lbs., pushing up to 50 lbs., standing, and walking. Feeling, grasping, hearing, and talking are required frequently (up to 75% of the workweek). Repetitive motions and visual acuity are required constantly (up to 100% of the workweek).

MINIMUM QUALIFICATIONS

Bachelor's degree in computer science or related field
Two (2) years of demonstrable and verifiable experience ~~supporting the hardware and systems infrastructure~~ in Information Technology infrastructure with a focus~~ed~~ 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

REVISED: Submitted:

07/01/2024 03/26/2024

JOB TITLE:	COORDINATOR CYBERSECURITY ADMINISTRATION
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

SCOPE OF RESPONSIBILITIES
Coordinates information security initiatives with internal stakeholders, vendors and auditors, for the purpose of protecting JCPS information systems and data. Monitors information security risks and enhances the district's cybersecurity posture by researching, recommending, implementing, testing, and managing information security best practices. Work both independently and with team members within the established procedures to protect against unauthorized system access, information modifications, and data destruction

PERFORMANCE RESPONSIBILITIES & EVALUATION CRITERIA
Serves as a member of the JCPS Cyber Security Operations Center (CSOC) which focuses on providing situational threat awareness and management of the district's security posture; the limited size of the JCPS cyber team will require that the CSOC collaborate effectively with other IT colleagues as well as external vendors as needed
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
Collaborates with other IT colleagues to review and test 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
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, 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
Routinely 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
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 trainings and other compliance requirements as assigned by the designated deadline
Regular, predictable performance is required for all performance responsibilities

This position requires collaboration, customer support, and team interaction

PHYSICAL DEMANDS

This work is conducted in an office setting. This position has inside environmental conditions with protection from weather conditions but not necessarily from temperature changes or atmospheric conditions while working on performance responsibilities.

This position requires the following physical activities rarely (up to 25% of the workweek): balancing, bending, climbing, crawling, crouching, driving, kneeling, and reaching. The following physical activities are required occasionally (up to 50% of the workweek): lifting up to 50 lbs., pulling up to 50 lbs., pushing up to 50 lbs., standing, and walking. Feeling, grasping, hearing, and talking are required frequently (up to 75% of the workweek). Repetitive motions and visual acuity are required constantly (up to 100% of the workweek).

MINIMUM QUALIFICATIONS

- Bachelor's degree in computer science or related field
- Two (2) years of demonstrable and verifiable experience in Information Technology infrastructure with a focus 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:	MANAGER DIGITAL PRIVACY AND CYBERSECURITY
DIVISION	TECHNOLOGY
SALARY SCHEDULE/GRADE:	II/GRADE 10
WORK YEAR:	220 DAYS
FLSA STATUS:	EXEMPT
JOB CLASS CODE:	
BARGAINING UNIT:	CLAS

Revised:
~~06/24/2020~~
3/27/2024

Submitted:
~~06/23/2020~~
3/26/2024

SCOPE OF RESPONSIBILITIES
Manages all procedures related to software requests throughout the district and assumes responsibility for ensuring all legal requirements are met. Manages ~~enterprise~~ district-wide security policies and systems. Develops, implements, and monitors the long-term information security strategy to achieve continued improvements in the district's information and systems security posture. Ensures compliance with the applicable security-related regulations, statutes, rules, and policies. Manages the JCPS Cyber Security Operations Center (CSOC) and directs the activities of that unit.

PERFORMANCE RESPONSIBILITIES & EVALUATION CRITERIA
Analyzes security metrics and other related reporting to elicit the district's information security risk profile and provides insightful advice to management for decision making
Performs enterprise-wide risk analysis and implements recommendations for application security, access control, and enterprise data safeguards to defend systems against unauthorized access, modification, or destruction
Coordinates with other IT staff as well as business units to conduct and review vulnerability security scans of systems to help identify and correct infrastructure security issues found in infrastructure and applications
Conducts district-wide awareness activities designed to assess compliance security policy education/enforcement to the entire workforce and leads committees to draft and recommend district-wide security and compliance policies and procedures
Leads the development, implementation, ~~and~~ enforcement, and regular review of the district's information security procedures, programs, and policies ~~and procedures and the ongoing management and oversight of all the district's information security procedures, programs, and policies~~
Drives the operationalization and oversees the ongoing management of the district's information security procedures, programs, and policies, holding both internal stakeholders and external vendors accountable for meeting their responsibilities
Participates in other security projects involving district information security, as needed, such as participating in compliance and risk meetings, reviewing vendor assessments for security requirements, etc
Establishes and enforces processes for developing security workflows
Coordinates, monitors, and tests the implementation of district-wide software and provides checkpoints to ensure digital privacy, safety, and security
Interfaces directly with District customers, vendors and other stakeholders and analyzes performance of the technology support services activities and documented resolutions, identifies problem areas, and devises and delivers solutions to enhance quality
Assumes responsibility for intake and fulfillment of district software vendor requests and maintaining FERPA, CIPA, COPPA, and/or other compliance requirements, regulations, and/or data protections
Works with internal and external district departments to compile and process documentation needed for data sharing agreements and contracts for software vendors
Participates in security incident responses as needed during or after business hours
Participates in projects, upgrades, outages and is available to assist after hours as needed by the team
Evaluates staff as assigned
Performs other duties as assigned by the designated supervisor
Completes all trainings and other compliance requirements as assigned and by the designated deadline

Regular, predictable performance is required for all performance responsibilities
This position requires collaboration, customer support, and team interaction

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 light weights.~~ This work is conducted in an office setting. This position has inside environmental conditions with protection from weather conditions but not necessarily from temperature changes or atmospheric conditions while working on performance responsibilities. This position requires the following physical activities rarely (up to 25% of the workweek): balancing, bending, climbing, crawling, crouching, driving, kneeling, and reaching. The following physical activities are required occasionally (up to 50% of the workweek): lifting up to 50 lbs., pulling up to 50 lbs., pushing up to 50 lbs., standing, and walking. Feeling, grasping, hearing, and talking are required frequently (up to 75% of the workweek). Repetitive motions and visual acuity are required constantly (up to 100% of the workweek).

MINIMUM QUALIFICATIONS
Bachelor's degree
Five (5) years of experience in ~~education or field of technology~~ Information Technology with a focus on cyber security and/or data privacy
Proficient user of technology with an understanding of risk management
Ability to lead the implementation of systems and processes to improve efficiency
Effective communication skills

DESIRABLE QUALIFICATIONS
Master's degree
A current, relevant, and industry-recognized certification or ability to complete department-designated certification(s)
Experience in a diverse workplace

JOB TITLE:	MANAGER DIGITAL PRIVACY AND CYBERSECURITY
DIVISION	TECHNOLOGY
SALARY SCHEDULE/GRADE:	II/GRADE 10
WORK YEAR:	220 DAYS
FLSA STATUS:	EXEMPT
JOB CLASS CODE:	
BARGAINING UNIT:	CLAS

Revised: 3/27/2024

Submitted: 3/26/2024

SCOPE OF RESPONSIBILITIES
Manages all procedures related to software requests throughout the district and assumes responsibility for ensuring all legal requirements are met. Manages district-wide security policies and systems. Develops, implements, and monitors the long-term information security strategy to achieve continued improvements in the district's information and systems security posture. Ensures compliance with the applicable security-related regulations, statutes, rules, and policies. Manages the JCPS Cyber Security Operations Center (CSOC) and directs the activities of that unit.

PERFORMANCE RESPONSIBILITIES & EVALUATION CRITERIA
Analyzes security metrics and other related reporting to elicit the district's information security risk profile and provides insightful advice to management for decision making
Performs enterprise-wide risk analysis and implements recommendations for application security, access control, and enterprise data safeguards to defend systems against unauthorized access, modification, or destruction
Coordinates with other IT staff as well as business units to conduct and review vulnerability security scans of systems to help identify and correct infrastructure security issues found in infrastructure and applications
Conducts district-wide awareness activities designed to assess compliance security policy education/enforcement to the entire workforce and leads committees to draft and recommend district-wide security and compliance policies and procedures
Leads the development, implementation, enforcement, and regular review of the district's information security procedures, programs, and policies
Drives the operationalization and oversees the ongoing management of the district's information security procedures, programs, and policies, holding both internal stakeholders and external vendors accountable for meeting their responsibilities
Participates in other security projects involving district information security, as needed, such as participating in compliance and risk meetings, reviewing vendor assessments for security requirements, etc
Establishes and enforces processes for developing security workflows
Coordinates, monitors, and tests the implementation of district-wide software and provides checkpoints to ensure digital privacy, safety, and security
Interfaces directly with District customers, vendors and other stakeholders and analyzes performance of the technology support services activities and documented resolutions, identifies problem areas, and devises and delivers solutions to enhance quality
Assumes responsibility for intake and fulfillment of district software vendor requests and maintaining FERPA, CIPA, COPPA, and/or other compliance requirements, regulations, and/or data protections
Works with internal and external district departments to compile and process documentation needed for data sharing agreements and contracts for software vendors
Participates in security incident responses as needed during or after business hours
Participates in projects, upgrades, outages and is available to assist after hours as needed by the team
Evaluates staff as assigned
Performs other duties as assigned by the designated supervisor
Completes all trainings and other compliance requirements as assigned and by the designated deadline
Regular, predictable performance is required for all performance responsibilities

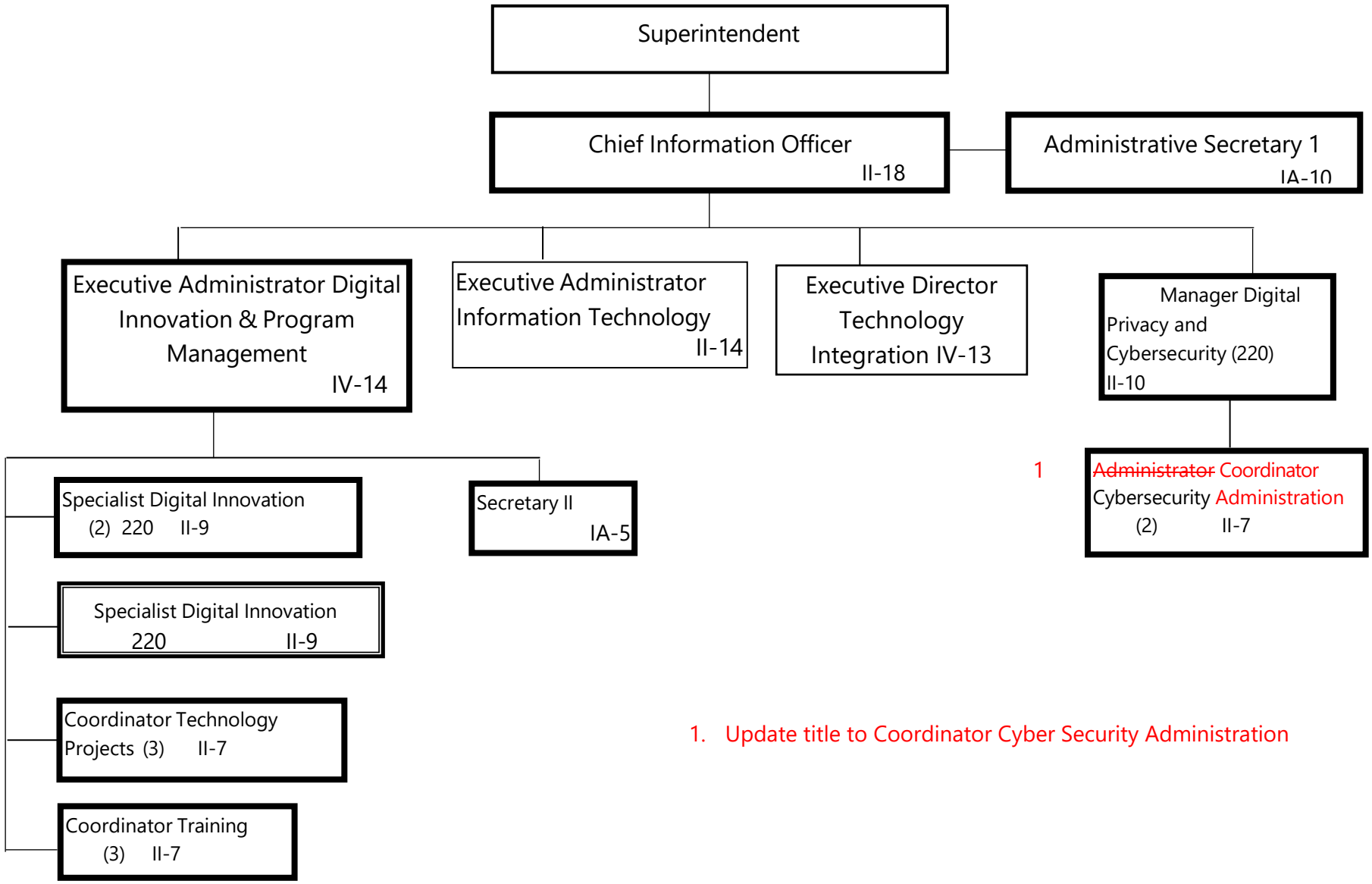
This position requires collaboration, customer support, and team interaction

PHYSICAL DEMANDS
This work is conducted in an office setting. This position has inside environmental conditions with protection from weather conditions but not necessarily from temperature changes or atmospheric conditions while working on performance responsibilities. This position requires the following physical activities rarely (up to 25% of the workweek): balancing, bending, climbing, crawling, crouching, driving, kneeling, and reaching. The following physical activities are required occasionally (up to 50% of the workweek): lifting up to 50 lbs., pulling up to 50 lbs., pushing up to 50 lbs., standing, and walking. Feeling, grasping, hearing, and talking are required frequently (up to 75% of the workweek). Repetitive motions and visual acuity are required constantly (up to 100% of the workweek).

MINIMUM QUALIFICATIONS
Bachelor's degree
Five (5) years of experience in Information Technology with a focus on cyber security and/or data privacy
Proficient user of technology with an understanding of risk management
Ability to lead the implementation of systems and processes to improve efficiency
Effective communication skills

DESIRABLE QUALIFICATIONS
Master's degree
A current, relevant, and industry-recognized certification or ability to complete department-designated certification(s)
Experience in a diverse workplace

Munis Unit No. TD1
Technology Division
~~2023-2024~~ 2024-2025



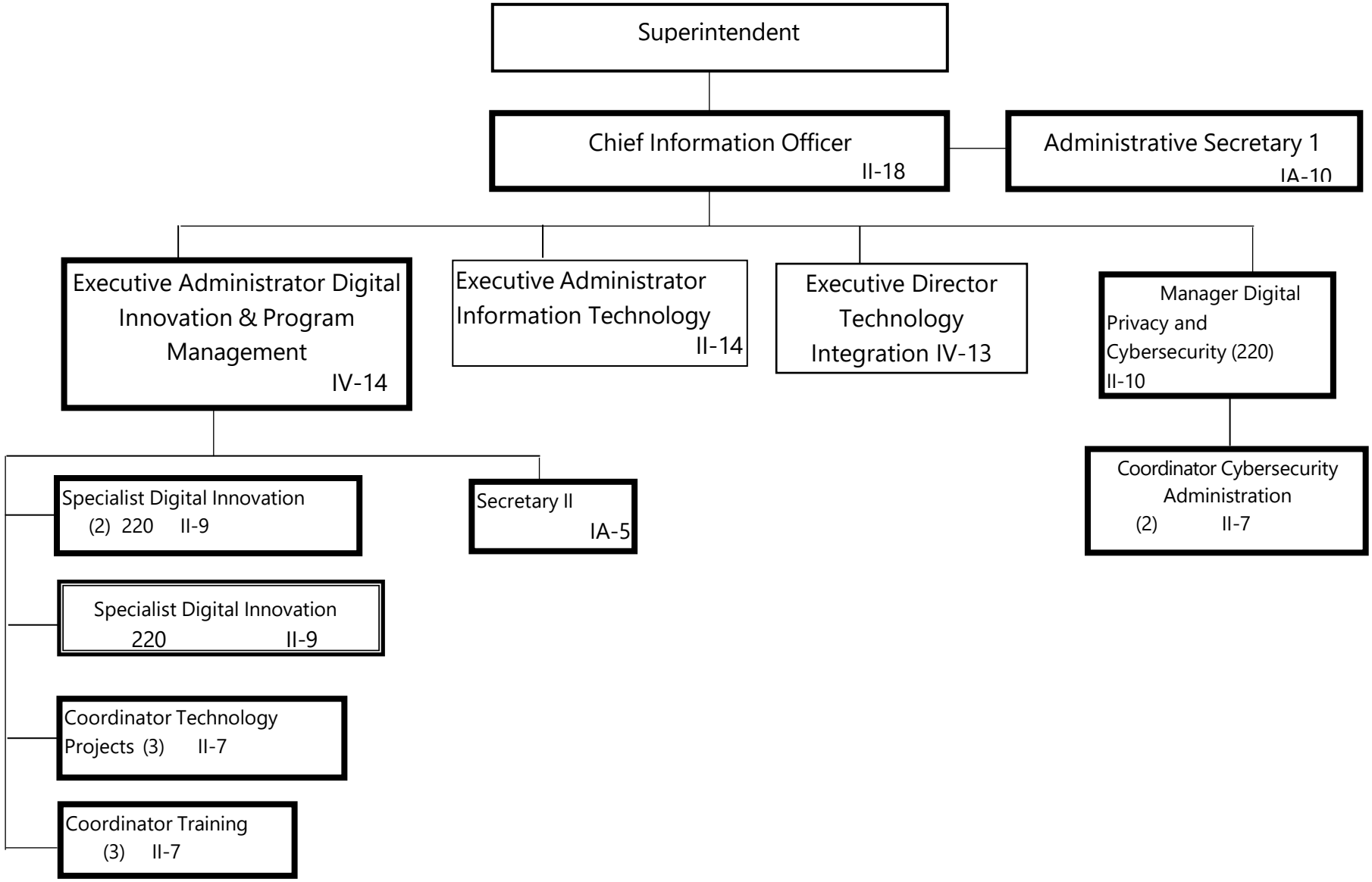
1. Update title to Coordinator Cyber Security Administration

Summary:

General Fund Positions: 15
Categorical Fund Positions: 1

Submitted: ~~03/28/2023~~ 03/26/2024
Effective: ~~03/29/2023~~ 07/01/2024

Munis Unit No. TD1
Technology Division
2024-2025

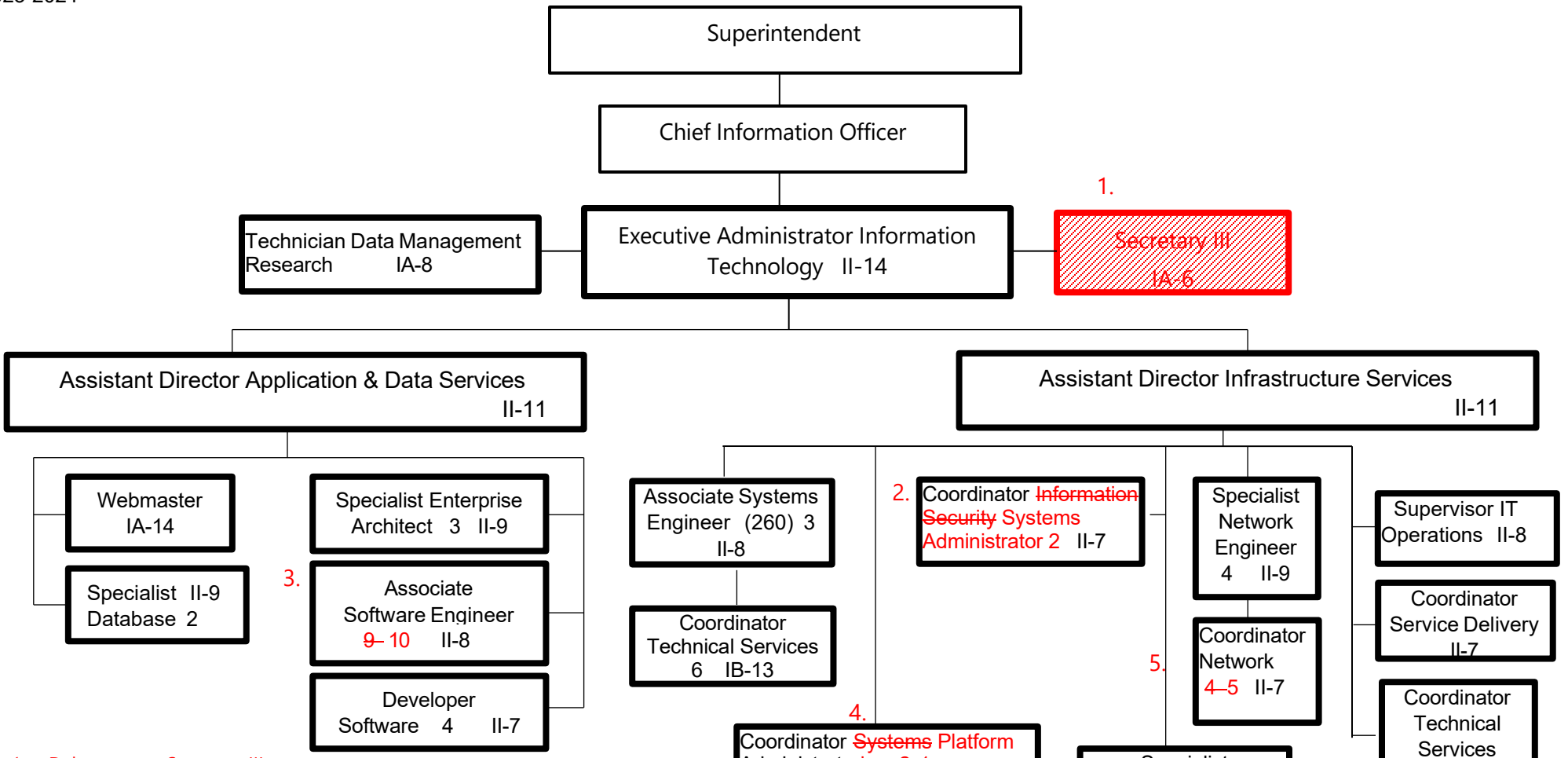


Summary:

General Fund Positions: 15
Categorical Fund Positions: 1

Submitted: 03/26/2024
Effective: 07/01/2024

Munis Unit No. MI1
Information Technology
2023-2024



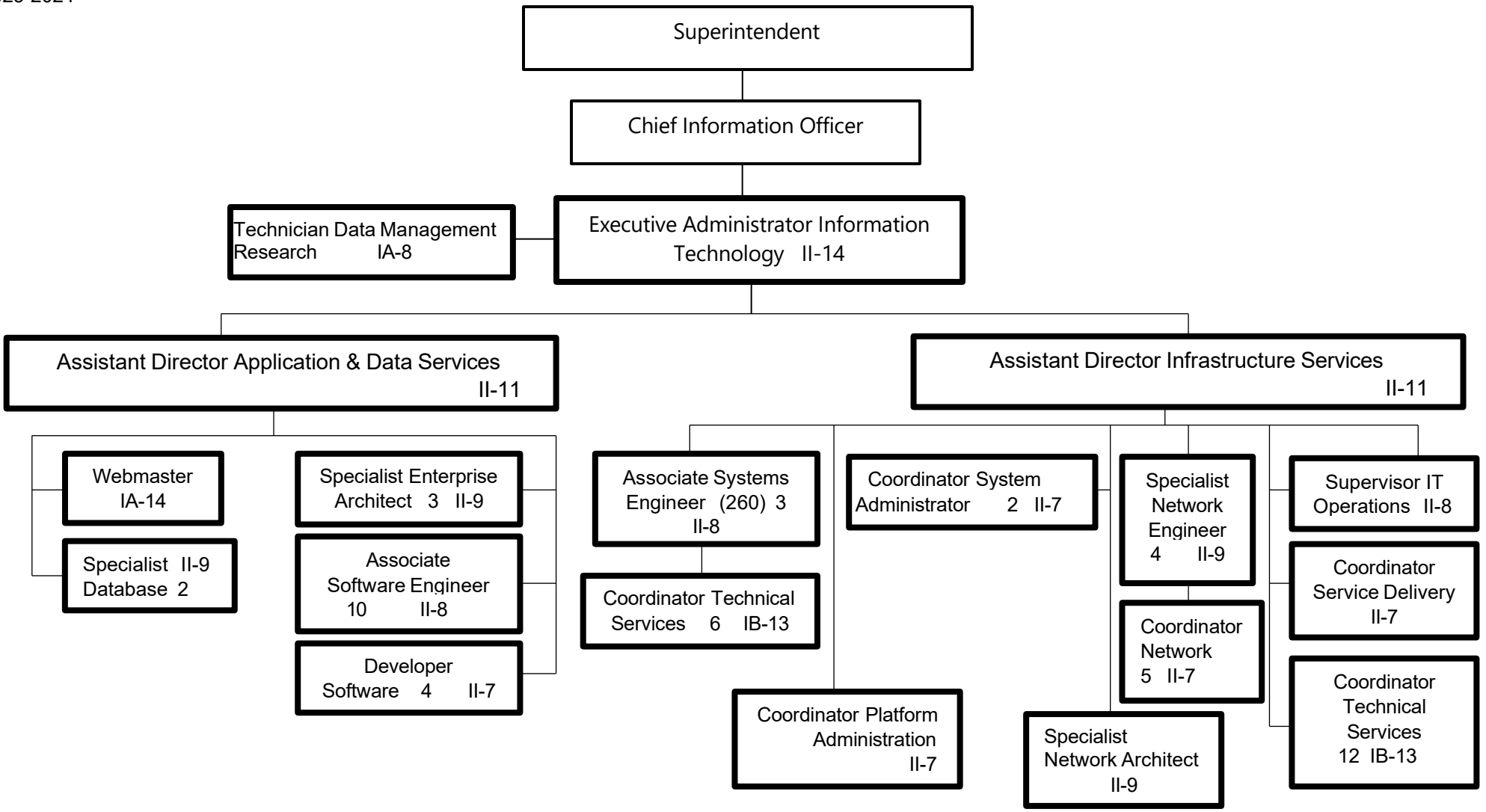
1. Delete vacant Secretary III
2. Update title to Coordinator Systems Administrator and add one (1) position
3. Add one (1) Associate Software Engineer
4. Update title to Coordinator Platform Administration and delete one (1) vacant position
5. Add one (1) Coordinator Network
6. Delete one (1) vacant Coordinator Technical Services

Summary:

General Fund Positions: 60
Categorical Fund Positions: 0

Submitted: ~~09/26/2023~~ 03/26/2024
Effective: ~~09/27/2023~~ 03/27/2024

Munis Unit No. MI1
Information Technology
2023-2024



Summary:

General Fund Positions: 60
Categorical Fund Positions: 0

Submitted: 03/26/2024
Effective: 03/27/2024