

Click one of these links to see the Job Description for that class:

Job Code	Title
S07033	Network Operations Center Technician
A07034	Network Operations Center Analyst
A07035	Network Operations Center Specialist
V07036	Network Operations Center Supervisor

Network Operations Center Series

S07033 -V07036

DESCRIPTION OF OCCUPATIONAL WORK

A Network Operations Center (NOC) is a centralized location or hub for servers and network elements simplifying information technology security and maintenance and allowing staff to monitor the performance and health of a network. The NOC serves as the first line of defense against network disruptions and failures. NOC personnel deploy, maintain, and resolve IP switching, remote access protocols, routing and firewalls using software, various tools and procedures, and monitoring systems.

This class series uses four levels to describe varied skilled, technical, and supervisory work. Positions perform network monitoring and technical analysis of system issues and outages as they occur across state enterprise networks and hardware. Work involves research to troubleshoot and resolve outages and network security issues, escalate to higher-level system and network administrators, or work with outside vendors or internal subject matter experts to resolve problems. The diversity of work responsibilities ranges from simple technical support to writing scripts and designing automated network functions to increase efficiency.

Job factors used in determining the level of NOC assignment include scope and difficulty of work performed, decisions/issues/problems managed, level of communication and collaboration with internal customers and external vendors, work directives received, and supervisory controls assigned.

Network Operations Center Technician

S07033

DISTINGUISHING CHARACTERISTICS: (A position is assigned to this class based on the scope and level of work performed as outlined below.)

This is the first level in the Network Operations Center series. Work is designed to train incumbents for a higher level in the class series. Although tasks are similar to those of a higher level, assignments are structured and performed with direction and assistance from others. Positions carry out established work processes and operations by learning to apply and follow procedures, techniques, rules, and regulations.

Decision making is limited with employees asking users pre-determined questions and following protocols based on established references. Judgment is needed in locating and selecting the most appropriate guideline, choosing from alternatives, and effectively communicating the necessary steps/actions to obtain the desired outcome.

Under general supervision, provides monitoring of network and system security, performance, and backup processes. Utilizes monitoring, alerting and ticketing tools to troubleshoot, report on and escalate issues as necessary. Provides off-hour Tier 1 Service Desk support for 24/7 state agencies. Assists in performing daily maintenance and back up procedures on various pieces of equipment. Follows, reviews, makes minor revisions, and maintains security procedures and practices related to network systems.

EXAMPLES OF WORK: (A position may not be assigned all the duties listed, nor do the listed examples include all the duties that may be assigned.)

Analyze, triage, and troubleshoot alarms related to network connectivity issues across a wide range of servers, routers, switches, and telecommunication equipment. Create tickets which categorize incidents based on alert type and severity to initiate response and track activity throughout resolution. Provide incident response by following written protocols and established communication practices.

Provide comprehensive Service Desk Tier 1 support to state users over the telephone, email, and messaging such as instant messaging. Manage the phone queue, taking direct support calls from users and document follow-up in the forms of incident or service requests in the ticketing system. Escalate incident or service requests to appropriate technical personnel when unable to resolve.

Monitor performance of network central processing units (CPUs). Deploy, maintain, and resolve IP switching, remote access protocols, routing, firewalls, and antivirus support.

Maintain reports on usage of bandwidth, utilization of servers, uptime, and other crucial elements.

Conduct backup and storage activities and follow disaster recovery protocols.

Assist in developing and maintaining Network Operations Center policies, procedures, and tools.

KNOWLEDGE, SKILLS, AND ABILITIES REQUIRED: (These are needed to perform the work assigned.)

Knowledge of: incident or service request ticketing systems and documentation practices; network monitoring systems and security fundamentals; business application software and operating systems; virtual private networks (VPNs); public agencies, services, and infrastructure. ITIL Service Management and Change Management. Lean Six Sigma.

Skill in: Service Desk and networking-based technology; documenting technological problems and actions taken to resolve problems; analyzing information and thinking in a logical manner.

Ability to: resolve user incidents or service requests through a ticketing system; troubleshoot network connectivity issues; attend to detail; prioritize work and handle multiple tasks simultaneously; consistently follow policies and procedures; perform basic root cause analysis; learn and keep current with technological advances; perform a variety of monitoring tasks, often changing assignments on short notice; effectively communicate over the phone, via email, instant messaging, mass notification and in person; investigate security incidents; effectively and consistently provide customer service and satisfaction.

MINIMUM QUALIFICATIONS: (Applicants will be screened for possession of these qualifications. Applicants who need accommodation in the selection process should request this in advance.)

High school diploma or equivalent. One year experience in data center operating environment, performing Service Desk functions or infrastructure support.

[LEGAL REQUIREMENTS:](#) (These qualifications are mandated by federal/state laws, statutes, and/or regulations.)

Not applicable.

[Return to Specification List](#)

Network Operations Center Analyst

A07034

[DISTINGUISHING CHARACTERISTICS:](#) (A position is assigned to this class based on the scope and level of work performed as outlined below.)

This is the second level of professional in the Network Operations Center series. Work requires general proficiency in network operations, security and user support and is conducted under limited supervision. Positions may troubleshoot problems that do not follow established patterns, so the cause is not obvious and established protocols do not work. Provides off-hour Tier 1 and some Tier 2 Service Desk support for 24/7 state agencies. Positions carry out defined work procedures and processes, using judgment to select the most appropriate technical guidelines and adapt them to accomplish new and complex tasks. Trains technical staff in standard policies and work processes.

Decision-making involves the same pre-determined questions and protocols; however, the complexity of decisions are greater involving program parameters, related protocols from other applications, timelines and personnel impacted by the decision. Judgment is used in escalating problems, contacting vendors or supervisors, communicating outage/remediation and emergency change information to users to maintain positive collaborative relationships, researching and planning various mitigation strategies, and documenting effective measures.

[EXAMPLES OF WORK:](#) (A position may not be assigned all the duties listed, nor do the listed examples include all the duties that may be assigned.)

Monitors a wide variety of information and network systems including, but not limited to, telecommunication circuits, LAN/WAN systems, routers, switches, firewalls, VoIP systems, servers, storage, backup, operating systems, and core applications using diagnostic programs on networks to pinpoint problems and monitor overall network health. Isolate potential security vulnerabilities and provide data analysis to assist in incident resolution.

Performs complex troubleshooting, fault isolation, root cause analysis, and incident management supporting IP networks and network hardware, ethernet, switches, routers, digital signaling, circuits, and related items/equipment. Resolves outages by isolating programs and escalating to appropriate technical personnel. Notify users and vendors of change management, issues, outages, and remediation status.

Respond to Tier 1 Level and limited Tier 2 Level Service Desk requests for technical support from state users. Prioritize incidents in accordance with agency business requirements, OCIO policies and operational impact.

Document all actions in accordance with standard policies and procedures.

Create and maintain reports on usage of bandwidth, utilization of servers, uptime/downtime, and other crucial elements.

Perform basic systems testing and operational tasks which may include installation of patches, network connectivity testing, script execution, etc.

Develop and document standard operating procedures for use by Network Operations Center staff including development of processes to ensure consistent execution of repeatable tasks.

KNOWLEDGE, SKILLS, AND ABILITIES REQUIRED: (These are needed to perform the work assigned.)

Knowledge of: IT network design, planning, and analysis; server operating systems and network devices; network monitoring systems and cyber security; business continuity and technology recovery principles and processes. ITIL Service Management and Change Management. Lean Six Sigma.

Skill in: diagnosing and resolving complex network switching and routing issues; using network monitoring and management tools in a large-scale environment; troubleshooting infrastructure problems/risks.

Ability to: troubleshoot with capture tools and network protocol analysis; define and create process documentation; communicate technical concepts to non-technical employees; manage and prioritize multiple incidents with potentially competing priorities; effectively communicate over the phone, via email, IM, mass notification and in person; serve as technological resource to others; make independent decisions after evaluating numerous alternatives; effectively and consistently provide customer service and satisfaction.

MINIMUM QUALIFICATIONS: (Applicants will be screened for possession of these qualifications. Applicants who need accommodation in the selection process should request this in advance.)

Associate's degree in computer science, information technology, or relevant field. Two years experience supporting and monitoring network systems or servers in an enterprise environment. Experience may be substituted for education on a year-for-year basis.

LEGAL REQUIREMENTS: (These qualifications are mandated by federal/state laws, statutes, and/or regulations.)

Not applicable.

[Return to Specification List](#)

Network Operations Center Specialist

A07035

DISTINGUISHING CHARACTERISTICS: (A position is assigned to this class based on the scope and level of work performed as outlined below.)

This is the third level of professional in the Network Operations Center series which commonly acts as a Subject Matter Expert (SME) for the NOC team. Work requires specialized proficiency in network operations, security and user support and is conducted under limited supervision. Positions develop and document solutions and internal instructions to improve processing tools and performance to reduce outages or downtime. Positions use judgment and resourcefulness to tailor existing guidelines so they can be applied to particular circumstances and deal with emergencies. Provides Tier 1 and Tier 2 Service Desk support for 24/7 Network Operations Center (NOC). Serves as a resource or guide by advising others on how to effectively use processes and tools within a system or as a member of a collaborative problem-solving team.

Independently researches the network or system activity, focusing on the analysis and design of systems to identify potentially troublesome configurations or security concerns. Work requires an expanded knowledge base of network systems and protocols, server maintenance and infrastructure. Incumbents at this level are responsible for the largest systems with the highest degree of impact and complexity. Monitors the performance and capacity of computer systems using a variety of tools. Determines cause for hardware, software and environmental alerts and malfunctions and documents follow-up processes and protocols for new events.

EXAMPLES OF WORK: (A position may not be assigned all the duties listed, nor do the listed examples include all the duties that may be assigned.)

Provides ongoing high-level technical monitoring for main systems and subsystems used by state agencies. Takes action to resolve or escalate alarms; reboots hardware and restarts services; acts as a technical escalation point for the Network Operations Center staff and support teams requiring assistance. Monitors open trouble incidents and ensures timely resolution.

Initiates short- and long-term in-depth analysis and investigation of network alerts/problems. Identifies problem and risk areas and advises supervisor of actions required to mitigate their impact.

Respond to Tier 2 Level Service Desk requests for technical support from state users. Prioritize incidents in accordance with agency business requirements, OCIO policies and operational impact. Maintains and updates technical documents to ensure the Network Operations Center knowledgebase is current.

Monitors weather and current events for the purpose of preparing for disaster response and alerting management to potential risks. Notifies management of major network outages and resolutions.

Reviews and technically modifies standard incident management and escalation processes utilizing past experience and subject matter expertise to reach timely and effective solutions to unusual and complex problems/issues which are not impacted/resolved by standard responses.

Independently research system or network activity to identify potentially troublesome configurations or security concerns. Writes scripts and designs automated network functions to increase efficiency and network performance.

Coordinates maintenance notifications and executes routing changes for circuits having maintenance performed.

Reviews and approves initial change management requests. Coordinates and facilitates change management meetings and activities.

KNOWLEDGE, SKILLS, AND ABILITIES REQUIRED: (These are needed to perform the work assigned.)

Knowledge of: network monitoring systems and cyber security including intrusion detection devices, firewalls, and anti-virus; server maintenance; enterprise monitoring tools; network routing principles and protocols; job control language and computer scheduling procedures. ITIL Service Management and Change Management. Lean Six Sigma certifications.

Skill in: maintenance of networks, LAN/WAN, routers, switches, servers, workstations, and applications; in-depth analysis, documentation, and decision resolution; diagnosing, researching, and resolving complex network and server problems.

Ability to: adapt established procedures to fit specific situations not covered by existing guidelines; train/orient technical personnel in a dynamic work environment; perform high level fault analysis including performance and capacity management; serve as technical advisor and mentor to others; perform system administration functions and manage day-to-day maintenance procedures; effectively communicate over the phone, via email and in person and work with users in high-stress situations.

MINIMUM QUALIFICATIONS: (Applicants will be screened for possession of these qualifications. Applicants who need accommodation in the selection process should request this in advance.)

Associate degree in computer science, information technology, or relevant field. Three years experience working in a Service Desk or Network Operations Center with networking equipment and protocols environments. Experience may be substituted for education on year-for-year basis.

LEGAL REQUIREMENTS: (These qualifications are mandated by federal/state laws, statutes, and/or regulations.)

Not applicable.

[Return to Specification List](#)

Network Operations Center Supervisor

V07036

DISTINGUISHING CHARACTERISTICS: (A position is assigned to this class based on the scope and level of work performed as outlined below.)

This is the fourth level of professional in the Network Operations Center (NOC) series assigned supervisory responsibilities for the NOC team. This level directly supervises technical and professional staff on the NOC team. At the Supervisor level, incumbents assume responsibility for scheduling, assigning, and directing the work of team members, identifying, communicating, and documenting work performance standards, ensuring compliance to project management timelines, and directing the implementation of policies, rules, and regulations.

Work involves setting overall goals and objectives for the Network Operations Center. Decisions are made at the operational level. Positions use judgement and resourcefulness to interpret circumstances in a variety of situations and establish guidelines that direct how work will be accomplished. This position oversees performance optimization, preventive maintenance and problem isolation/resolution through planning and analysis, design, development, and recovery best practices.

EXAMPLES OF WORK: (A position may not be assigned all the duties listed, nor do the listed examples include all the duties that may be assigned.)

Responsible for the overall planning, organizing and execution of Network Operations Center operations. Supervises the monitoring and support of agency systems, including networks, data centers, servers, PC's, operating systems, and associated hardware. Establishes support capacity through planning, allocation of NOC staff, budgeting, procurement, and deployment of appropriate technology solutions.

Interview, hire, supervise, develop, evaluate, and discipline Network Operations Center staff and support personnel. Oversee successful delivery of tasks, assignments, and NOC projects.

Ensure the efficient utilization of NOC resources, including personnel and resources, across the State. Manage staffing levels for the NOC and recommend new resources based on organizational and user demands.

Develops and maintains processes with escalation paths to ensure issues are handled promptly. Adapts, integrates, and modifies existing monitoring systems to manage NOC requests across all state agencies. Establishes procedures, priorities, and standards for NOC operations. Ensures compliance with OCIO, state and contractual guidelines, requirements, and policies.

Works across state agencies on strategic initiatives to improve security, expand adoption of platform and infrastructure as a service, and make continued improvements to disaster recovery capabilities. Develops project timelines, project plans, and checklists to ensure schedules are achieved within budgetary constraints. Creates and maintains project documentation and provide project status updates.

Communicates changes, enhancements, and modifications through written documentation to users, managers, administration, and other stakeholders, so that issues and solutions are understood. Maintain a wide array of performance metrics and key performance indicators regarding service delivery and customer satisfaction.

ITIL Service Management and Change Management support and management.

Business Continuity and Disaster Recovery development, implementation, and management.

KNOWLEDGE, SKILLS, AND ABILITIES REQUIRED: (These are needed to perform the work assigned.)

Knowledge of: management principles involved in strategic planning, resource allocation, leadership techniques, and the coordination of people and resources; budget and financial management practices; enterprise infrastructure hardware and applications, networks, systems, data center operations; security technologies and applications; ideologies, techniques and tools for quality assurance, process improvement and best practices. ITIL Service Management and Change Management. Lean Six Sigma certification.

Skill in: effective communication and collaboration skills; project planning and problem-solving; time management; critical thinking to solve problems, plan strategically, and foster innovation.

Ability to: adapt in response to new information, changing conditions, or unexpected obstacles; receive and give constructive feedback to others; effectively listen and process information provided by others; make sound, well-informed, and objective decisions.

MINIMUM QUALIFICATIONS: (Applicants will be screened for possession of these qualifications. Applicants who need accommodation in the selection process should request this in advance.)

Bachelor's degree in computer science, information technology, or relevant field. Two years' experience supervising or leading an IT Service Desk team or Network Operations Center environment. Experience may be substituted for education on year-for-year basis.

LEGAL REQUIREMENTS: (These qualifications are mandated by federal/state laws, statutes, and/or regulations.)

Not applicable.

[Return to Specification List](#)

SPECIAL NOTES APPLICABLE TO ALL LEVELS:

Work requires sitting at a computer for extended periods of time, viewing monitor screens and receiving/making phone calls.

Certification related to the area of assignment and technological operations may be required.

State agencies are responsible to evaluate each of their positions to determine their individual overtime eligibility status as required by the Fair Labor Standards Act (FLSA).

Established: <1/2022>

Note: Classification-specification is subject to change. Please refer to the Nebraska State Personnel Job Specification website at <https://das.nebraska.gov/personnel/classcomp/jobspecs/jobspecs.html> to ensure this represents the most current copy of the description.

The following is a summary of changes made to this class specification.

Section	Change Description	Effective Date