

Employee's Signature \_\_\_\_\_ Date \_\_\_\_\_

Supervisor's Signature \_\_\_\_\_ Date \_\_\_\_\_

**POSITION PURPOSE:**

The Security Administrator will support all Metropolitan State University enterprise applications by troubleshooting and resolving any related technical issues, tuning the applications for maximum response and performance time, performing change control activities related to the production environment. This person is expected to perform security audits of networked systems and applications on a quarterly basis. He/she will be responsible for performing security compliance audits related to MnSCU security guidelines and will be the point person for all security related support.

**REPORTABILITY:**

Reports to: Director of Technical Services.

Supervises:

**DIMENSIONS:**

Clientele: All Metropolitan State University faculty, staff and students who are using network services from any of the university's campuses or remotely. Also interacts with MnSCU technical support staff as well as various hardware/software vendors.

Principal Responsibilities, Tasks and Performance Indicators

SECURITY ADMINISTRATOR

P	%	D
A	40	A

**I. Provide system analysis and design input for all server systems to address security requirements from MnSCU, FERPA, etc.**

- A. Provide secure network and server services to Metropolitan State University clientele.
- B. Responsible for testing server backup and restore operations, including offsite storage of tapes and software.
- C. Analyze new applications and confirm that new software adheres to MSU/MnSCU security standards.
- D. Responsible for all system software updates and security patches.
- E. Work with D2L support staff to support students and faculty with D2L access.
- F. Monitor Network security using appropriate software and tools.
- G. Maintain, update, and expand disaster recovery documents.
- H. Presents updated disaster recovery document bi annually to IT Management.
- I. Respond promptly to reported security violations received from students and from other campus departments and organizations outside the University.
- J. Ensure MSU all operating systems and email systems are protected from viruses, spam, spyware, and malware.
- K. Evaluate all new software requirements set forth by other state agencies (MAPS, SEMA4, SCUPPS, PALS etc.)

**Technical Performance Indicators:**

- Ensures complete data protection by verifying backup integrity quarterly.
- All MSU servers and network devices adhere to MnSCU security guidelines.
- Network equipment and servers have recent software updates and patches.
- Users report acceptable service accessibility from remote locations.
- System applications are kept current and accessible to authorized users.
- Disaster recovery documents are presented to IT management on time.

NETWORK ADMINISTRATION

P	%	D
A	25	A

**II. Manages the network system administration, analysis, design for numerous server systems (20+) to address the needs and requirements of students, faculty and staff.**

- A. Provide quality network and server services to Metropolitan State University clientele.
- B. Analyze and assess needs for university network infrastructure and recommend priorities to IT management.
- C. Define and document procedures for installation of new hardware and software.
- D. Responsible for server backup and restore operations, including documentation and offsite storage of tapes and software.
- E. Research and introduce new applications and adapt commercial software for compatibility with Metropolitan State University's IT infrastructure.

- F. Responsible for all network software updates and security patches.
- G. Analyze and develop network security and maintenance procedures.
- H. Oversees the monitoring of the university’s network activity and directs the adjustments of network traffic to ensure efficient operations
- I. Work with the Administrative Technology Support Specialist to evaluate all new software requirements set forth by other state agencies (MAPS, SEMA4, SCUPPS, PALS etc.)

**Technical Performance Indicators:**

- Ensures complete data protection by verifying backup integrity on a regular basis.
- Network equipment and servers have recent software updates and patches.
- Recommendations are made to the IT managers that are compatible with current systems conform to current standards.
- Downtime due to network component failures are kept to a minimum to ensure maximum output.
- System applications are kept current and accessible to authorized users.
- Listens well and asks appropriate questions.

SOFTWARE APPLICATIONS

P	%	D
A	15	A

**III. Support and enhance Metropolitan State University’s network software applications.**

- A. Plan, Implement, and maintain a network intrusion detection system.
- B. Plan, Implement, and maintain an anti-spam solution for the college mail system.
- C. Firewall configuration is reviewed biannually and report is presented to IT Management.
- D. Develop and implement regular network scanning procedures to identify compromised computers.
- E. Install, test, upgrade, and maintain University’s network application software.
- F. Create, and maintain accurate and up-to-date log of Metropolitan State’s current security risks.
- G. Administer and document the university’s firewall access-lists.
- H. Meet with faculty and staff to determine proper software configurations.
- I. Assist the Network Administrator in the network capacity planning and design of new and expanded network technology.

**Technical Performance Indicators:**

- MSU data network is secure and all security incidences are thoroughly documented.
- Processes are documented and shared with IT management and AQIP coordinator.
- Users report low levels of unauthorized commercial email.
- Network software is fully documented in both electronic and hardcopy formats and all changes to network are incorporated when implemented.
- Ability to organize and prioritize work to achieve established timeline

P	%	D
A	10	A

**V. Provide tier III technical support for IT staff, and operational support.**

- A. Serve as lead worker to IT Desk, support staff, and student employees during second shift.
- B. Provide technical expertise to in the areas of desktop and server security to desktop and network support

**INFORMATION TECHNOLOGY SPECIALIST 3  
(Network Security Administrator)**

**PCN#1087506**

- staff.
- C. Respond to individual user network problems and inquiries - research problems, identify and implement solutions in a timely manner.
- D. Help support staff install, configure, and test new software.
- E. Assist in the Planning, configuration, and installation of software for computer classrooms and labs (e.g., Technical Communication, Math, ICS, Mac and PCs) as required.
- F. Provide third level assistance to desktop support staff on exceptional and challenging problems.
- G. Document security processes for university AQIP initiative.

**Technical Performance Indicators:**

- Communicate compatibility of software and security solutions with IT staff on a regular basis.
- Specialized software is tested and provided as requested.
- Takes initiative to research, resource, resolve and be self-reliant when approaching projects and tasks.
- User problems are resolved in a timely fashion.

CUSTOMER SERVICE

P	%	D
A	5	A

**V Assist and enhance computer lab utilization and exhibit excellent customer service skills with students, staff, faculty and peers.**

- A. Communicates effectively, in writing, verbally and non-verbally, with IT staff and managers.
- B. Builds positive and effective relationships with IT staff and internal/external customers.
- C. Listen and asks appropriate questions.
- D. Follows directive and priorities established by IT managers in a timely and effective manner.
- E. Instruct and orient students, faculty, and staff in the procedures and policies involved in using the computing center facilities.
- F. Instruct and assist users working on supported Metropolitan State University hardware and software.

**Technical Performance Indicators:**

- Users experiencing difficulty are assisted promptly.
- Users get appropriate assistance in using the hardware.
- Faculty gets appropriate assistance in software evaluation and use of network software.
- Misuse of equipment is reported promptly.
- Problems are researched, discussed and resolved in a timely manner.
- Takes initiative to research, resource, resolve and be self-reliant when approaching projects and tasks
- Builds positive and effective relationships with IT staff and internal/external customers
- Willingness to cooperate with others to accomplish objectives and work towards common goals.
- Effectively communicates in writing, verbally, non-verbally and interpersonally.
- Listens well and ask appropriate questions. Keeps supervisor and co-workers informed.

PROFESSIONAL DEVELOPMENT

P	%	D
B	5	A

**VI Increase knowledge and experience with support of computing by working with all aspects of work in the IT department.**

**INFORMATION TECHNOLOGY SPECIALIST 3  
(Network Security Administrator)**

**PCN#1087506**

- A. Be available to supervisor, CIO and the IT department to assist with major hardware and software projects.
- B. Assist supervisor, other management staff and CIO with special projects as needed.
- C. Focus self-development on learning about advanced computing and networking topics.
- D. Develop and implement a personal staff development plan.
- E. Stay current in Information Technology through electronic journals, seminars, Computer Based Training, On-line help, documentation, and discussion groups.
- F. Attend seminars and workshops to keep current with changes hardware and software.
- G. Participate in newsgroups and listservs to collaborate and communicate with other universities and colleagues.
- H. Seeks out and engages in learning to develop understanding of continuous improvement tools and skills, develop professionally and in preparation for future opportunities to better serve the university.
- I. Participates in training to improve understanding and skills for continuous improvement of processes.

**Technical Performance Indicators:**

- Demonstrations and information are shared with Information Technology Staff.
- Problems and tips are shared on Information Technology staff listserv.
- Makes changes and suggests changes to improve systems and processes.

Professional journals are shared with other interested colleagueNATURE AND SCOPE (relationships, knowledge, skills and abilities; problem solving and creativity; and freedom to act).

**Relationships:**

The employee will interact with all levels of staff (support, professional, management and faculty) and hardware/software vendors as needed. The ability to work as a team member to accomplish goals within the established timeframes is required. The employee will also be in communication with technical staff outside the university. Ensuring excellent working relationships with these groups will aid the successful delivery of LAN services.

**Knowledge, Skills and Abilities:**

This position requires in-depth technical background with extensive knowledge and experience in networking concepts and components. In-depth experience with Linux, Novell NetWare, Windows 2003 server, , and TCP/IP are required. Current working knowledge and experience in network concepts and configuration and troubleshooting of firewalls, Systems, and email are required.

The employee must have the ability to communicate technical information to both technical and non-technical personnel. The position requires good written documentation skills so as to create network documentation plus excellent interpersonal skills are required. Current experience in Windows XP, Windows 2003 Server, Novell Netware, Linux, and the ability to coordinate software compatibility solutions. Regular attendance is an essential function of this position.

Leadership skills and the ability to assign schedule and train other staff.

**Required: Education/Experience = a bachelor's degree plus 3-5 years of current working experience in Networking and/or Network security; OR relevant industry certifications plus 4 - 6 years of current working experience in Networking and/or Network Security.**

The incumbent must possess knowledge in network design, analysis, and operational principles and practices as well as ability to manage large and complex production projects with limited technical input from management.

Fundamental knowledge of project management is a must.

**Problem Solving:**

**INFORMATION TECHNOLOGY SPECIALIST 3  
(Network Security Administrator)**

**PCN#1087506**

Solving problems on a daily basis is necessary part of this position. The employee must be able to take initiative to research and solve problems in different software/hardware situations. The incumbent must be able to make short and long-term decisions based on a variety of criteria including established priorities, budget restrictions, technology changes, and available resources. Demonstrates a commitment to continuous improvement by engaging in activities alone or with others to improve university processes for the benefit of students and other stakeholders.

**Freedom to Act:**

This position works under very limited supervision, and has the ability to make decisions independently. The individual in this position must be able to take a problem and design a complete plan for solving that problem, regardless of time or difficulty and pursue solutions and issues to complete resolution. Realizing objectives and priorities, in view of the many interruptions that will occur in this position, will demand that the individual be free to act in a variety of ways. General guidance and direction will be available both on a regularly scheduled basis and when requested.

---

*This description is intended to indicate the kinds of tasks and levels of work difficulty that is required of the position. It is not intended to limit or modify the right of the supervisor to assign, direct and control the work of the employee. The use of particular expressions or illustrations describing duties shall not be held to exclude other duties that are of similar kind or level of difficulty.*