

Position Description

IS Enterprise Network Services Specialist

Position Summary

The Division of Enterprise Technology provides statewide information technology services utilizing a combination of both State-owned equipment and vendor-provided services. The division ensures the effective and efficient use of information technologies in support of Wisconsin government services and programs. It designs, administers, promotes, and supports information technology services to state agencies, local governments, tribal governments, private partners, schools, universities, libraries, and citizens.

Under the general review of the Network Access Management Section Chief/Unit Supervisor, this position functions as a technical expert for the enterprise network security infrastructure. This position is responsible for the integration and connectivity of very complex, disparate distributed network security infrastructure for agencies and enterprise systems. These systems involve multiple hardware and software platforms, multiple application systems, and advanced, emerging technologies such as load balancing, Global name load balancing, and Access control via F5 and F5 modules, Next Generation and Web Application Firewalls (WAF), Cloud Access Security Broker (CASB), and enterprise proxy configurations. This position is responsible for the research, development, and support of core enterprise network infrastructure and tools to control network security between devices connected to the state network.

This position supports security-based network hardware for all major, complex IT systems in all state agencies. The position also will participate in projects from genesis through implementation and completion. The incumbent will frequently work on projects and tasks that require strong customer service skills, good communication skills and the ability to work within a team approach. The ability to function with an enterprise perspective and to work with technical staff, DET management, and other entities' staff on technical design and business issues is critical.

This position is accountable for the quality of service provided to state agencies and other partners. This position also provides on call technical hardware and software support of the infrastructure environment that supports the very complex and critical application systems 24x7x365.

Goals and Worker Activities

35% A. Provide advanced technical support, technical administration for enterprise proxy, web Application firewall (WAF) and other Network Access Management (NAM) infrastructure

A1 Research, install, test and implement security hardware such as Next Generation Firewalls, F5 and other security appliances for access to vital business applications/devices.

A2 Maintain installed enterprise firewalls, F5 and F5 Modules, WAF, other NAM physical/virtual security hardware, system software, on an ongoing basis to remain at recommended release level and to resolve problems in order to maintain system stability.

- A3 Maintaining multi-site network operations and software applications, operation systems and regular maintenance with both private and public facilities.
- A4 Lead the fulfillment of agency requests for network services as assigned through the service request process.
- A5 Direct the use of procedures along with developing, establishing, and documenting procedures for the proper use and support of enterprise network hardware and software.
- A6 Lead and participate in the development, documentation, and implementation of IT management best practices to ensure the quality of services delivered to customers and partners.
- A7 Participate with vendors providing server hardware and software management and other infrastructure services to ensure procedures are being followed and program goals are achieved.
- A8 Ensure that published IT management policies and best practices in such areas as Service Delivery and Service Support are being followed.
- A9 Monitor network data and make recommendations to better utilize resources for optimal performance and cost-effectiveness.
- A10 Maintain change records of tuning, updating, and patching changes made and their affect resource.
- A11 Maintain metrics to measure and evaluate utilization of resources for all Network Access Management physical or virtual enterprise IT infrastructure systems and usage.
- A12 Oversee and lead Disaster Recovery documentation creation, modification, and testing

30% B. Provide technical consulting and technical direction for enterprise proxy, F5 and F5 Modules, WAF, and other Network Access Management services.

- B1 Provide direction for use of procedures along with developing, establishing, and documenting procedures for the proper use and support of enterprise security network hardware and software.
- B2 Fulfill agency requests for network security services as assigned through the service request process.
- B3 Actively lead and participate in the development, documentation and implementation of IT management best practices to ensure the quality of services delivered to customers and partners.
- B4 Ensure that published IT management policies and best practices in such areas as Service Delivery and Service Support are followed.
- B5 Provide oversight with vendors providing server hardware and software management and other infrastructure services to ensure procedures are being followed and program goals are achieved.
- B6 Work with security to develop and implement sound security practices and policies that balance the need for security and accessibility of business applications.

B7 Lead in Disaster Recovery documentation creation, modification, and testing

25% C. Participate in complex IT projects to implement and maintain enterprise and agency specific server infrastructure and systems.

- C1 Develop and use divisional project management policies, procedures, and practices in leading teams in implementing complex infrastructure components and enterprise applications.
- C2 Tech lead project teams to help them understand and follow enterprise information portfolio management policies, procedures, and practices.
- C3 Lead project teams under the direction of a project manager as assigned
- C4 Provide quality service and maintain positive working relationships with customers
- C5 Provide network infrastructure consulting to customers, agencies, and enterprise services.

10% D. Continually update technical skills and participate in the Employee Development Program and other duties.

- D1 Maintain familiarity with activities and trends in the infrastructure hardware and software and other related technologies.
- D2 Seek out and attend appropriate training courses, conferences and seminars.
- D3 Read technical publications to maintain a high level of technical knowledge concerning data processing hardware and software with emphasis on shared infrastructure technology.
- D4 Lead co-workers in activities of professional and technical associations to contribute to the development in the data processing industry and in various agencies of government.
- D5 Perform other assigned tasks not specifically enumerated.

Knowledge, Skills, and Abilities

1. Ability to function as a leading team member, including the open sharing of information, willingness to help wherever needed, and an understanding that team and the organization's objectives supersede personal agendas.
2. Ability to communicate clearly and effectively to both technical peers and less technical customers in person and via written media such as email, reports, and project charters.
3. Ability to learn quickly; synthesize complex information, identify key points and communicate results accurately and effectively.
4. Ability to develop and mentor staff in the skills required for the senior position.

5. Resourceful in identifying and obtaining information sources needed to perform duties effectively.
6. Knowledge that IT exists not for its own sake but for the business value it brings.
7. Advanced knowledge of and ability to perform technology and product research, testing, installation, customization, troubleshooting and support.
8. Advanced knowledge of remote network security administration which included installation, administration and troubleshooting experience.
9. Advanced knowledge TCP/IP, DNS, DHCP, WINS and other common network protocols.
10. Advanced knowledge of network security management concepts and software such as next generation firewalls, VPN, and different security tools.
11. Knowledge of open source systems software alternatives to purchased software.
12. Advanced knowledge of application security concepts surrounding protocol protection, sequel protection, code protection for technologies such as WebSphere, IIS, apache, Tomcat, and databases (like Microsoft SQL, Oracle, and DB2 type calls)
13. Knowledge of Maintaining, administering, and updating cloud firewalls and CASB services in Amazon or Azure and security policies surrounding clouds solutions via key tools, such as Firemon.
14. Advanced knowledge of installing, updating, and configuring Firewalls (such as Palo Alto or Cisco) and their accompanying management tools (Panorama and/or Cisco Security Manager).
15. Knowledge of Installing, maintaining, updating, and configuring Web Application Firewalls (WAF), either by direct coding or by Dynamic Applications Security Testing (DAST) tools' output.
16. Knowledge to support the installs, migrations, and upgrades of F5 reverse proxy suite, including Application Security Monitoring, Load-Balancing, Global Load-Balancing, and Application provisioning Monitor.
17. Knowledge to write, support, and administer rule policies to control application communication to and from the internet, agency headquarters, and remote branch offices.