TECHNOLOGY SECURITY ADMINISTRATOR

SUMMARY/PURPOSE

The Technology Security Administrator's role is to ensure the secure operation of technology based data systems and maintain compliance with legislative and regulatory requirements. This includes checking server and firewall logs, examining network traffic, establishing and updating security policies, and troubleshooting. This position will also analyze and resolve security breaches and vulnerability issues in a timely and accurate fashion, and conduct user activity audits where required.

ESSENTIAL DUTIES AND RESPONSIBILITIES (other duties may be assigned)

1. Develop and institute security and compliance goals and objectives.
2. Review proposed technology projects to identify potential risks.
3. Audit existing technology security practices across the organization, isolate potential risks or liabilities, and develop mitigation plans.
4. Develop, implement, maintain, and oversee enforcement of policies, procedures and associated plans for system security administration, and user system access based on industry-standard best practices.
5. Assist in the design and implementation of disaster recovery plan for operating systems, databases, networks, servers, and software applications.
6. Assess need for any minor or significant security reconfigurations and execute them if needed.
7. Keep current with emerging security alerts and issues.
8. Conduct research on emerging products, services, protocols, and standards in support of security enhancement and development efforts.
9. Recommend and implement disaster avoidance and impact reduction strategies as they relate to information technology.
10. Assess IT purchases to ensure they support security and compliance mandates.
11. Coordinate and facilitate consultation with stakeholders to define business and system security requirements for new technology implementations.
12. Interact and negotiate with vendors and contractors to obtain protection services and products.
13. Recommend, schedule, and perform security improvements, upgrades, and/or purchases.
14. Track and measure the enterprise's technology risk posture.
15. Manage securing of all platforms and centralize security event management.
16. Develop and deliver risk awareness training for key staff and stakeholders.
17. Ensure that information security measures adhere to all applicable laws and regulations.
18. Assist in the configuration and maintenance of security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and anti-virus software.
19. Maintain the security of data transferred both internally and externally.
20. Design, perform, and/or oversee penetration testing of all systems in order to identify system vulnerabilities.
21. Design, implement, and report on security system and end user activity audits.
22. Monitor server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity. Interpret activity and make recommendations for resolution.
23. Recommend, schedule (where appropriate), and apply fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach.
24. Download and test new security software and/or technologies.
25. Keep current with emerging security alerts and issues.
26. Provide security and compliance guidance to members of the IT team.

JOB REQUIREMENTS

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the knowledge, skills, and abilities required.

1. Education & Experience Requirements
   - A. Graduation from an accredited technical school or college/university with a degree in the field of computer science, plus two years of progressively responsible, verifiable experience in network security; or
   - B. Five years of full-time, verifiable experience in network security; or
   - C. A combination of verifiable education and experience equaling five years.
   - D. Certifications in CPTC, Security+, CEH, or other related certifications are desired.

2. Knowledge Requirements
   - A. Knowledge of risk management principles and models.
   - B. Proven experience in audit of legislative and/or regulatory compliance.
   - C. Knowledge of laws, legislation, regulations, and applicable practices pertaining to the public sector, public safety, and credit card processing industries.
   - D. Experience in technical management of technology software and hardware platforms.
   - E. Understanding of the organization's goals and objectives.
   - F. Broad hands-on knowledge of firewalls, intrusion detection systems, anti-virus software, data encryption, and other industry-standard techniques and practices.
   - G. In-depth technical knowledge of network, PC, and platform operating systems, including CISCO, Microsoft Windows, and Linux.
   - H. Working technical knowledge of current systems software, protocols, and standards.
   - I. Hands-on experience with devices such as firewalls, switches, and routers.

3. Skill Requirements
   - A. Proven leadership and management skills.
   - B. Highest levels of personal and professional integrity.
   - C. Superior analytical and problem-solving abilities.
   - D. Excellent written, oral, and interpersonal communication skills.
   - E. Highly self- motivated and directed.
   - F. Team-oriented and skilled in working within a collaborative environment.
   - G. Strong organizational skills.
   - H. Excellent attention to detail.

4. Ability Requirements
   - A. Ability to effectively prioritize and execute tasks in a high-pressure environment.
   - B. Ability to present ideas in both business-friendly and IT-friendly language.
   - C. Ability to create and maintain a positive working environment that welcomes diversity, ensures cooperation, and promotes respect by sharing expertise with team members, fostering safe work practices, and developing trusting work relationships.

5. Physical Ability Requirements
   - A. On-call availability and periodic overtime to meet project deadlines.
   - B. Light travel may be required.
   - C. Sitting for extended periods of time.
   - D. Dexterity of hands and fingers to operate a computer keyboard, mouse, and other computer components.
   - E. Ability to attend work on a regular basis.
   - F. Ability to transport oneself to and from City of Duluth facilities.

HR: LD	Union: Basic	EEOC: Professionals	CSB: 05/03/2016	Class No:
WC: 8810	Pay: 141	EEOF: Admin/Finance	CC:	Resolution: