

# IT Cyber Security Engineer

JOB TITLE: IT Cyber Security Engineer

FLSA STATUS: Non-exempt

GRADE: 41

DEPARTMENT: Technical Services

APPROVED DATE: 09/2010

REVISED DATE: 09/2021, 02/2017, 12/2018, 02/2022

## Job Summary

Work with Information Technology Services Management to develop and drive security initiatives, improve the cyber security posture of the Library, and manage technical risks.

This position contributes to the Library District's effective operation, providing library services, spaces, and resources that are representative of diverse cultures and perspectives, intentionally inclusive, and accessible to everyone.

## We Value Lived Experience

Sno-Isle Libraries is committed to embedding equity into our organization. As we engage in equity work, it's important to have a good foundation to frame the work and then provide training opportunities to build skills and knowledge.

We value and embrace the unique experiences our staff members bring to the organization and recognize how their experiences improve the service we provide.

## Essential Functions

*Functions listed are intended only as illustrations of the various types of work performed. The omission of specific duties does not exclude them from the position if the work is similar, related or a logical assignment to the position. Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions of this job.*

1. Design, build and maintain security solutions, platforms and infrastructure. This include researching, evaluating and testing emerging cyber security threats, trends, tools and capabilities and providing recommendations on what emerging technologies should be assimilated, integrated and introduced within Sno-Isle Libraries to ensure IT capabilities respond to the Library's business strategy.

2. Respond to security incidents. Gather, analyze, and present forensic evidence of malware, intrusions, and breaches. Perform analysis seeking, identifying and confirming cyber threats, risks and vulnerabilities to all Sno-Isle systems and infrastructure. This includes conducting vulnerability scans on a routine and ad-hoc basis.
3. Lead the development and deployment of cyber security processes, procedures, projects and initiatives.
4. Perform risk analysis of proposed capabilities for new and existing systems and infrastructure resulting in specific technical recommendations for improving security and/or mitigating cyber risk.
5. Communicate with technical and non-technical staff about cyber security issues, threats, vulnerabilities and risk reduction strategies.
6. Receive and process requests for support services related to the position's area of responsibility. This includes determining the urgency of service requests for continuity of customer service, suggesting actions to users to overcome technical problems, and diagnosing the issue for assignment to appropriate staff. Work closely with other IT staff as needed to gather information to respond, track and follow-up on requests to ensure that issues are resolved.
7. Develop and manage vendor relationships related to cyber security on behalf of Sno-Isle Libraries.
8. Work with IT Management to develop, enhance and maintain Disaster Recovery, including regular testing of the Sno-Isle IT Disaster Recovery Plan.
9. Work with IT Management to develop the mission and vision of Library cyber security services to foster a service-oriented culture and growth mindset driven by continual service improvement techniques.
10. Assist in the development of the cyber security strategy and roadmap, and ensures its integration with the overall Library and IT strategic plans.

### **Additional Duties and Responsibilities**

1. Perform Unix/Linux system administration.
2. Establish and maintain effective relationships and networks with colleagues locally, regionally and nationally.
3. Participate in a rotating schedule of providing weekend technical support to library staff.

4. Attend meetings, trainings, conferences and workshops as assigned to maintain the high level of technical competence needed to perform the duties required.
5. Assist with special projects as required.
6. Perform other duties as assigned.

## **Supervision**

The position reports to the IT Enterprise Infrastructure & Operations Manager. The position does not supervise the work of others; but may be required to lead project teams.

## **Knowledge, Skills, and Abilities**

1. Strong customer service and communication skills.
2. Demonstrated ability to work cooperatively and maintain effective working relationships with others.
3. Ability to uphold the principles of equity, diversity, and inclusion in the workplace and the community.
4. Ability to communicate effectively with diverse audiences.
5. Ability to work cooperatively and maintain effective interpersonal skills with the public and co-workers.
6. Ability to communicate computer concepts and terminology with other staff.
7. Ability to investigate and diagnose complex problems in a multi-platform environment and to develop effective solutions.
8. Advanced working knowledge of LAN/WAN hardware, SD-WAN, network theory, and Internet protocols.
9. Ability to secure applications, systems, servers, data and LAN/WAN network infrastructure.
10. Working knowledge of information security issues, trends and leading practices.
11. Self-discipline and self-motivation required.

## **Education and Experience**

*Knowledge, skills, and abilities for this position can be acquired by a combination of experience and education including:*

1. A Bachelor's degree is required. A Bachelor's degree in computer science or related field is preferred.
2. At least five years of experience working with network systems support and configurations.
3. At least three years of cyber intrusion detection, incident response or forensic analysis experience required.
4. Linux and Windows system administration experience required.
5. Coding/scripting experience e.g., Perl, Bash, VB Script, Python, etc. required.
6. Security oriented certifications such as CISSP, GCIA, CEH, GCIH, GCFA or CSIH preferred.

### **Physical and Environmental Conditions**

The physical demands described here are representative of those that must be met by a staff member to perform the essential functions of this job successfully. Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions.

Most of the work is carried out within a generally accessible, safe, indoor environment. While performing the duties of this job, the incumbent is required to operate computers for extended periods of time. The incumbent must be able to operate hand tools, move equipment or materials weighing up to 50 pounds and must be able to set up equipment used in training and demonstration.

The incumbent must regularly communicate with coworkers and members of the public. These contacts and situations are deemed to be generally safe and free of undue stress, but require incumbents to be cordial, helpful, and skilled in interpersonal relations with others both in the public and within the Library District.