

**Position Title:** Information Systems and CyberSecurity Analyst

**Reports to:** Director of Information Technology

**Category:** Non-Exempt

**Status:** Regular Full-Time

**Position summary:**

The primary function involves safeguarding information system assets by identifying and solving potential and actual security problems as well as the maintenance and administration of security applications within the Information Technology (IT) Department and other departments throughout the credit union. Emphasis will be on Microsoft network operating systems, hosted online exchange with Azure, Cisco Meraki firewalls, various endpoint and RMM solutions and network security systems and applications.

**Tasks:**

Responsibilities include, but are not limited to the following:

- Protects system by defining access privileges, controls structures and resources identifying abnormalities and reporting violations
- implements security violations and inefficiencies by conducting periodic audits
- Develop security standards and best practices for the organization
- Support the credit union's local area and wide area network hardware and software to ensure that back end functions, systems, PCs, servers, and all peripheral products are operational.
- Recommend security enhancements to management
- Educates users of potential threats and good business practices
- Implements and maintains security controls
- Documents technical support issues
- Supports the Helpdesk to resolve problems for end users
- Performs other duties as assigned.

**Basic Qualifications:**

- Be willing to learn and adapt in a fast paced, ever changing, growing financial institution.
- Candidate must be outgoing and able to perform quality work independently.
- Must hold a valid state driver's license.
- Periodic lifting of up to thirty-five pounds will be occasionally required.
- Sufficient manual dexterity to work with hand tools and computers.
- Must be able to stand, crouch, and climb to perform various types of manual labor while working on computers.
- Work environment involves exposure to potentially dangerous situations concerning electrical shock, cuts, and minor burning.



**Preferred Skills/Experience:**

- Associate's degree in Computer Science, Information Systems or equivalent education or work experience
- Minimum of three (3) + years of prior relevant experience in Cyber Security; advanced certifications such as SANS GIAC/GCIA/GCIH, CISSP or CASP and /or SIEM-specific training and certification a plus
- Experience with Microsoft Office (Outlook, Word, Excel), SharePoint, Office 365.
- Certification in Cyber Security and Cisco technologies preferred
- Windows Servers.
- Proficient with Windows networking
- Hosted Exchange / Azure80 administration
- Experience supporting routers and switches
- Operational experience with Jack Henry and Associates Symitar Epyxis a plus

X \_\_\_\_\_  
Employee Signature Date

X \_\_\_\_\_  
Manager Signature Date