Job Description: Security Specialist

Position Title: Security Specialist
Department: Technology
Reports To: Director of Technology Infrastructure and Security

---

Position Summary

The Security Specialist supports the credit union's physical and information security programs by providing day-to-day operational support, monitoring, and maintenance of security systems and tools. This role works closely with the Director of Technology Infrastructure and Security to ensure a safe and secure environment for employees, members, facilities, and information assets. The Security Specialist plays a key role in security incident response, access management, and the ongoing reliability of both cybersecurity and physical security technologies.

Key Responsibilities

Operational Security Support

- Provide day-to-day operational support for the credit union's security tools, including endpoint protection platforms, vulnerability scanners, identity and access management systems, SIEM dashboards, and other enterprise security technologies.
- Perform routine monitoring to identify anomalies, alerts, and system health issues, escalating concerns according to established procedures.

System Maintenance & Monitoring

- Assist the Director of Technology Infrastructure and Security with the maintenance, configuration, tuning, and lifecycle management of all security systems, ensuring optimal performance and alignment with industry best practices.
- Conduct regular reviews of log data, system alerts, and event notifications to support proactive threat detection and incident prevention.

Endpoint & Application Security

- Ensure all security applications deployed on employee computers and servers are properly installed, up-to-date, and functioning as intended.
- Coordinate patching, updates, and troubleshooting of endpoint security software, including antivirus, encryption, and monitoring agents.

Help Desk Security Support

- Manage and respond to help-desk tickets related to security applications, access requests, and user-reported security concerns.

- Provide timely troubleshooting, issue resolution, and documentation of findings or escalations.

Physical Security Administration

- Maintain and manage building security systems, including fob access controls, intrusion alarms, environmental monitoring sensors, and door hardware.
- Oversee the operation, configuration, and upkeep of video surveillance systems (CCTV), ensuring proper placement, retention settings, and video quality.
- Coordinate with facilities teams and outside vendors to address repairs, upgrades, and new installations.

Cross-Functional Support

- Serve as a backup to the Director of Technology Infrastructure and Security for operational tasks, incident response, vendor coordination, and reporting activities.
- Participate in security assessments, audits, and compliance reviews as needed.
- Assist in maintaining security procedures, documentation, incident logs, and system inventories.

Security Awareness & Compliance

- Support the delivery and tracking of security awareness programs, phishing simulations, and user-training initiatives.
- Help ensure organizational adherence to regulatory requirements, internal policies, and industry best practices.

Qualifications

Required

- Associate's degree in Information Security, Information Technology, or a related field; or 1-2 years equivalent experience.
- Working knowledge of cybersecurity principles, physical security systems, and endpoint protection technologies.
- Strong troubleshooting and analytical skills.
- Ability to manage multiple priorities in a fast-paced environment.
- Excellent communication and documentation skills.

Preferred

- Experience working in a financial institution or regulated environment.
- Familiarity with NCUA/FFIEC security expectations.

- Certifications such as Security+, CySA+, CCNA Security, or equivalent.
- Experience with access control systems, video management platforms, and SIEM tools.

Competencies

- **Attention to Detail** – Carefully monitors systems, logs, and alerts to identify risks.
- **Integrity & Confidentiality** – Handles sensitive information responsibly.
- **Problem Solving** – Quickly diagnoses and resolves security-related issues.
- **Collaboration** – Works effectively with IT, Facilities, Compliance, and other departments.
- **Proactive Mindset** – Anticipates threats and recommends improvements.