Prairie Land Electric Cooperative
Job Description & Requirements

Title: **Cybersecurity Specialist**
Department: Information Technology and Technical Services
Classification: Hourly, Full-Time, Non-Exempt
Reports To: Director of Technical Services
Supervises: N/A

Core Values:

PLEC is committed to upholding the following core values:

- **Safety** – Hold our employees to the highest safety standards to provide a safe working environment at all times.
- **Respect** – Be professional and considerate in all situations
- **Integrity** – Act with honesty and transparency in all we do
- **Unity** - Show commitment, dedication, trustworthiness, selflessness, and dependability, while working together to achieve our mission.
- **Accountability** – Hold ourselves and others accountable while inspiring others to achieve highest standards.

Job Summary

The goal is to cultivate a strong cybersecurity culture within the Cooperative by actively engaging management and maintaining regular communication with employees through training sessions and interactive initiatives. Strengthening the Cooperative's security framework involves monitoring and safeguarding its networks, computer systems, and data from potential threats. This includes installing and maintaining security software, establishing baseline configurations, documenting identified security incidents, and implementing best practices. As a subject matter expert, the Cybersecurity Specialist is expected to remain well-informed about the latest intelligence and evolving hacker methodologies.

Responsibilities

- Secure both IT and OT networks.

- Collaborate with stakeholders to define, develop, implement, and maintain the company's security framework (policies, standards, guidelines, and procedures) based on the needs and requirements of each department.

- Conduct research and provide recommendations on solutions, designs, or architecture to harden the Cooperative's current posture.

- Develop, document, and verify security baseline configurations on Cooperative-owned assets.

- Perform audits to validate adherence and implement new controls of the company's security framework.

- Evaluate environment to design, implement, enhance and manage a zero-trust network.
- Create a culture of security awareness by leading and enhancing cyber safety training.
- Maintain and manage the Security Information and Event Monitoring solution to monitor server logs, firewall logs, and network traffic for unusual or suspicious activity.
- Conduct threat hunting on any anomalous behavior (blue/purple team activity) and lead remediation efforts.
- Administrate and maintain the endpoint detection and response solution.
- Monitor the security systems for anomalous traffic patterns.
- Perform risk assessments and testing of enterprise technology infrastructure.
- Manage vulnerability scanning and provide recommendations to mitigate discovered vulnerabilities.
- Analyze Cooperative business requirements and provide objective advice on the use of enterprise security solutions.
- Facilitate penetration testing and follow through with all mitigating actions.
- Manage and maintain physical access within the access control system.
- Implement security improvements by assessing current situations and evaluating trends.
- Work with all Cooperative employees to realize enterprise approach to security.
- Encourage cyber security awareness and implementation of best practices by third parties accessing enterprise infrastructure to minimize risk to the Cooperative.
- Understand the latest hacker techniques and propose appropriate countermeasures.
- Learn all aspects of the IT and OT networks and systems to support and secure them
- Assist in other IT duties and special projects, as necessary.
- Promote cyber safety culture by partnering with Management staff to further the Cooperative Strategic Plan.

Other Duties:

Please note this job description is not designated to cover or contain a comprehensive listing of activities, duties, or responsibilities that are required of the employee for this job. Duties, responsibilities, and activities may change at any time with or without notice.

Education and Experience

- Bachelor’s degree in Cybersecurity, Information Technology, or other related IT field, or 5 years related experience and/or training or equivalent.

Required Skills and Abilities

- Must be able to maintain professionalism and control under all circumstances.
- Proficient in Microsoft Office products including Excel and Word.
- Strong verbal, written, analytical and interpersonal skills.
- Ability to dissect and resolve complex problems quickly and systematically.
- Organized, keen attention to detail, and efficient.
- Ability to conduct research into IT security issues and products as required.
- Analytical/logical thinking ability.
- Ability to assemble facts in a clear, understandable manner.
- Team-oriented and skilled in working within a collaborative environment.
- Maintain high level of confidentiality with regards to associate, member-owner, and corporate information.
- Possess effective techniques to research and access all sources necessary to fulfill position responsibilities.

Environment:

Work is in a controlled office environment. Office environment includes sedentary work with normal temperatures and normal conversation noise levels.

Physical Demands:

Physical exertion is minimal. Normal activity requires sitting, standing, or walking. Lifting is limited to normal office routine and items carried or lifted will range between 1 and 20 pounds. To successfully carry out the duties of the position, the use of computer equipment, calculators, and occasional use of copiers. Occasional travel by automobile or airplane is necessary.