YOUR NEXT CHAPTER STARTS HERE!

Niagara Peninsula Energy Inc.

JOB TITLE: Cybersecurity Analyst

Niagara Peninsula Energy Inc. (NPEI) is a trusted Ontario electricity distributor serving approximately 59,000 customers across Niagara Falls, Lincoln, Pelham and West Lincoln. Rooted in community and focused on performance, NPEI is entering a period of significant growth and opportunity shaped by electrification, modernization, customer expectations and a focus on new non-regulated businesses. To drive innovation, shape culture and innovate people, join NPEI as our new Cybersecurity Analyst.

WHY THIS ROLE MATTERS

Because this is a rare opportunity to influence the future of a respected community utility at a time of major sector transformation

Because you will join an organization that values safety, customer-centricity, accountability, collaboration and community impact

Shape Strategy. Drive Transformation. Power the Future of Energy!

ROLE SUMMARY

The Cybersecurity Analyst reports to the Vice President, Information Technology and is responsible for safeguarding Niagara Peninsula Energy's information assets, operational technology environments, critical infrastructure, and sensitive customer and corporate data from evolving cybersecurity threats. The role leads the identification, assessment, monitoring, and mitigation of cyber risks through the implementation, administration, and continuous improvement of security controls designed to prevent unauthorized access, data compromise, service disruption, and asset loss. The Cybersecurity Analyst conducts risk and vulnerability assessments, threat analysis, and security monitoring activities to proactively identify risks that may impact information systems, operational continuity, and business processes. In addition, the position supports regulatory compliance, incident response, security awareness, and cyber resilience initiatives, ensuring alignment with the Ontario Energy Board Cyber Security Framework, industry best practices, and Niagara Peninsula Energy's enterprise risk management objectives.

MAJOR ROLES & RESPONSIBILITIES

1. Evaluate, recommend, implement, and manage cybersecurity technologies, controls, and programs that support the Corporation's strategic objectives, regulatory requirements, and evolving security needs.
2. Collaborate with IT and business stakeholders to ensure security architecture, design standards, and cybersecurity principles are consistently applied across all technology initiatives and operational environments.
3. Implement, monitor, and continuously improve security controls, including the identification, documentation, assessment, and remediation of security risks, vulnerabilities, and control gaps. Provide timely analysis and recommendations to the Vice President, Information Technology.
4. Perform regular security assessments, internal and external vulnerability scans, and penetration testing activities to ensure the confidentiality, integrity, and availability of corporate information assets, infrastructure, applications, and data repositories. Analyze findings and support remediation planning and implementation.
5. Administer, support, and optimize the Security Information and Event Management (SIEM) platform, ensuring security events, audit logs, and monitoring data are reviewed, investigated, and escalated as required.
6. Develop and deliver cybersecurity performance metrics and reports aligned with corporate KPIs, including security incidents, vulnerabilities, compliance status, threat trends, privileged access management, and security control effectiveness. Review system access rights, audit logs, and encryption standards and recommend corrective actions where necessary.
7. Maintain current knowledge of cybersecurity threats, emerging technologies, industry best practices, and regulatory requirements to proactively identify opportunities for improving the Corporation's cybersecurity posture.
8. Contribute to cybersecurity strategy development and annual planning activities, including budget recommendations, technology roadmaps, risk mitigation initiatives, and security program enhancements.
9. Monitor and analyze alerts generated by monitoring, detection, and endpoint management platforms for both Information Technology (IT) and Operational Technology (OT) environments, escalating significant events and risks as required.
10. Support the development, testing, maintenance, and continuous improvement of disaster recovery, incident response, cyber resilience, and business continuity programs, including participation in tabletop exercises, red team engagements, and cybersecurity simulation activities.
11. Conduct vulnerability assessments and coordinate remediation activities by tracking risk exposure, monitoring mitigation progress, and reporting on compliance with the Corporation's Vulnerability and Patch Management Program.
12. Collaborate with external cybersecurity service providers, managed security partners, and third-party monitoring organizations to investigate threats, assess emerging risks, and provide technical expertise on cybersecurity-related projects and initiatives.
13. Investigate cybersecurity incidents and events, coordinate containment and remediation activities, and proactively collect, analyze, and communicate threat intelligence and security-related information to stakeholders.
14. Monitor intrusion detection and prevention systems, endpoint security solutions, and network security controls, analyze findings, and recommend corrective actions to improve security effectiveness and reduce organizational risk.
15. Support and promote the Corporation's Cybersecurity Education and Awareness Program by monitoring participation, measuring effectiveness, identifying gaps, and recommending initiatives to strengthen the organization's security culture.
16. Support compliance with the Ontario Energy Board Cyber Security Framework, industry standards, and internal security policies through ongoing assessments, documentation, evidence collection, and audit support activities.
17. Participate in cybersecurity and technology projects to ensure security requirements are identified and incorporated throughout system design, implementation, integration, and operational support activities.
18. Performs tasks as assigned

WHAT YOU WILL BRING

- Strong written and verbal communication skills
- Knowledge of cyber security processes and network protocols.
- Knowledge of disaster recovery planning and penetration testing and execution.
- General knowledge of technical hardware and network applications.
- Ability to work effectively with IT colleagues, in a collaborative environment
- Ability to configure security and cybersecurity solutions, following designs, and infrastructure
- Ability to adapt to a constant changing environment.
- Strong organization, technical and time management skills.
- Ability to analyze complex problems and utilize problem solving techniques to derive solutions
- Ability to recognize and deal with sensitive issues in a discreet and professional manner.
- Strong attention to detail
- Understanding of management philosophies, techniques, and problem-solving methods.
- Basic knowledge of Occupational Health & Safety requirements as it relates to individual, organizational and operational requirements.

YOUR EXPERIENCE

- Bachelors degree in Computer Science or College Diploma in Information Technology/Security.
- Certified Information Security Manager (CISM) is an asset.
- Requires 2 – 5 years of relevant, progressive experience.

APPLY TODAY!

SALARY RANGE: **$92,727 - $115,909**

Interested and qualified applicants are encouraged to apply by submitting a cover letter and resume no later than by **4:30 p.m. on October 6, 2026** to people.culture@npei.ca

Please attach your resume and cover letter in **.docx or .pdf format**.

Niagara Peninsula Energy Inc. is committed to creating an inclusive workplace and we encourage candidates from diverse backgrounds, experiences, and those who may need accommodation to apply to join our team. Our commitment to excellence in diversity goes beyond promoting equity. By incorporating a variety of experiences and perspectives, we create opportunities for innovative solutions and maximize the impact of our work.

We sincerely thank all applicants for their interest in this position; however, due to volume, only those selected for an interview will be contacted. Niagara Peninsula Energy Inc. is an equal opportunity employer and is AODA compliant. If you are selected to participate in the recruitment process for the position to which you have applied and require a disability-related accommodation, please notify the People & Culture Department. Any personal information submitted will be managed in accordance with the requirements of the Municipal Freedom of Information and Protection of Privacy Act and will be used only to determine eligibility for employment. In accordance with Canadian immigration requirements, this advertisement is directed to applicants who are authorized to work in Canada.