IT SECURITY MANAGER

Niagara Peninsula Energy Inc. (NPEI) is seeking a qualified individual to join our management team in the position of IT Security Manager. This position is an in-office role working out of our corporate office located in Niagara Falls, with occasional travel to all NPEI locations where our corporate technical infrastructure is in place. This position reports to the Vice President, IT, Cybersecurity and Business Application Support and supervises the Senior IT Security Analyst as well as the IT Security Analyst. Designated as Chief Information Security Officer (CISO), the IT Security Manager is responsible for the successful execution of the Written Information Security Program along with adhering to the design and implementation of IT solutions to protect NPEI assets from unauthorized access, compromise or loss in accordance with the Ontario Energy Board (OEB) Cyber Security Framework.

Primary Duties & Responsibilities:

- Manage and lead the Corporate Written Information Security program for IT networks and Operation Technology to ensure the confidentiality, integrity and availability of the data residing on or transmitted to/from/through the Corporation's workstations, servers, and other systems and in databases and other data repositories.
- Lead the development of security control assessments for common platforms/devices. Plan and lead the implementation of findings from said assessments to ensure changes take into account security components, risks and management of security and cybersecurity products and programs to ensure alignment with the strategic goals of the organization, as well as, mitigation that cyber-security measures do not negatively impact business functions.
- Configure, manage and administer the implementation of the Security Information and Event Monitoring platform, ensuring audit trails, system logs and other monitoring data are reviewed and actionable.
- Manage the design and execution of internal and external scans including vulnerability assessments, penetration tests and security audits.
- Review complex analyses on intrusion detection system results and implement recommendations of corrective actions.
- Facilitate Incident Response (IR) activities as a Subject Matter Expert (SME) through the incident response life cycle and report corrective action plans to the Corporation's internal governance committee.
- Participates in the strategic planning and prepares the budgeting requirements for cyber security.
- Assess the results of the Remote Monitoring and Management Infrastructure alerts to determine the risks and prepares remediation plan related to all IT and OT assets.
- Ensure completeness of IT Security documentation to validate that all IT and OT assets are inclusive of all IT managed asset inventory lists, network diagrams, process maps and data flow charts.
- Develop the audit plan of the comprehensive IT and OT disaster recovery plan, the incident response plan and assist in the development and maintenance of the Corporate business continuity plans. This includes regularly scheduled Red team exercises and playbook simulations.
- Develop, maintain, and administer the vulnerability Patch Management Release Program in collaboration with the IT Manager.
- Develop and oversee the Corporation's Cyber Security Education and Awareness Program.
- Develop and review reports, that outline security and cybersecurity risks across the organization. Ensure reports align with the Corporation's security KPI's. and can be used to implement standards and

procedure of analysis to input into incident reports and Root Cause Analyses in support of a known incident or cybersecurity breach.

Required Qualifications & Skills:

- Bachelors Degree in Computer Science or College Diploma in Information Technology/Security.
- Certified Information Security Manager (CISM) is highly preferred.
- Certified Information Systems Security Professional (CISSP) would be an asset.
- Requires a minimum five (5) years of relevant, progressive experience in a supervisory role.
- Work experience in an electric utility is an asset.
- Experience with the National Institute of Standards and Technology (NIST) Cyber Control Set.
- Advanced working knowledge of cyber security administration and network protocols.
- Advanced working knowledge of disaster recovery planning and penetration testing and execution.
- Strong attention to detail and the ability to prepare accurate reports, documentation and diagrams.

How to Apply:

Interested and qualified applicants are encouraged to apply, in confidence, by submitting a cover letter and resume by email addressed to: people.culture@npei.ca no later than **4:30 p.m. on Friday, March 29, 2024.**

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.