Indigenous.Link

Canada's fastest growing Indigenous career portal, Careers.Indigenous.Link is pleased to introduce a new approach to job searching for Indigenous Job Seekers of Canada. Careers.Indigenous.Link brings simplicity, value, and functionality to the world of Canadian online job boards.

Through our partnership with Indigenous.Links Diversity Recruitment Program, we post jobs for Canada's largest corporations and government departments. With our vertical job search engine technology, Indigenous Job Seekers can search thousands of Indigenous-specific jobs in just about every industry, city, province and postal code.

Careers.Indigenous.Link offers the hottest job listings from some of the nation's top employers, and we will continue to add services and enhance functionality ensuring a more effective job search. For example, during a search, job seekers have the ability to roll over any job listing and read a brief description of the position to determine if the job is exactly what they're searching for. This practical feature allows job seekers to only research jobs relevant to their search. By including elements like this, Careers.Indigenous.Link can help reduce the time it takes to find and apply for the best, available jobs.

The team behind Indigenous.Link is dedicated to connecting Indigenous Peoples of Canada with great jobs along with the most time and cost-effective, career-advancing resources. It is our mission to develop and maintain a website where people can go to work!

Contact us to find out more about how to become a Site Sponsor.

Corporate Headquarters:
Toll Free Phone: (866) 225-9067
Toll Free Fax: (877) 825-7564
L9 P23 R4074 HWY 596 - Box 109
Keewatin, ON P0X 1C0

Job Board Posting

Careers.Indigenous.Link

Date Printed: 2024/04/26

Specialist, Security Policy & Audit

Job ID	**o8N5jfw3-12652-5732**	
Web Address	https://careers.indigenous.link/viewjob?jobname=o8N5jfw3-12652-5732	
Company	EPCOR	
Location	Edmonton, Alberta	
Date Posted	From: 2022-06-22	To: 2050-01-01
Job	Type: Full-time	Category: Utilities

Description

Highlights of the job

We are hiring a full-time permanent Specialist, Security Policy & Audit position working out of Edmonton, AB. The Security Policy and Audit Specialist reports to and works closely with the OT Systems & Security Senior Manager.Ã‚Â As the Security Policy and Audit Specialist, you work with other specialized cross-functional groups and design, document, build, and measure EPCOR Distribution and Transmission, Inc. (EDTI) wide cyber security policies. You provide process expertise, manage and update documentation, and collect/present evidence for EDTI focused aspects of the Alberta Reliability Standards (ARS) Cybersecurity Infrastructure Protection (CIP) Standards regulatory requirements. Additionally, you coordinate EPCOR-wide cyber security requirements to ensure ongoing consistent and accurate evidence collection and presentation to demonstrate compliance.Ã‚Â As a strong communicator and collaborator, you work alongside the OT Security Specialist analyzing highly technical documentation including firewall and SIEM logs, network and infrastructure design documentation, OT/SCADA equipment configuration, and detailed product technical documentation, in order to design, build, and support EDTI's broader cyber security program and relevant controls.Ã‚Â This position may be eligible for our hybrid work program!What you'd be responsible for

Providing input to the OT Systems & Security team's plans and directions, and demonstrating ongoing relationships with other positions, as required.Ensuring all EDTI OT assets are properly inventoried and categorized by risk, with appropriate policies in place to ensure that systems are configured and monitored to protect EPCOR's operational computing and communications infrastructure from malicious attacks and/or unintended changes.Leading a cross-functional group of SMEs, managing and maintaining EPCOR's NERC/ARS CIP policies covering information classification, change management, access management, electronic security perimeter, physical security, malicious software prevention, security testing, ports and services management, patch management, security incident response, disaster recovery, audit evidence collection, and other applicable activities through ongoing and yearly update and review processes.Overseeing compliance sustainment and continuous improvement efforts associated with EPCOR's ARS CIP compliance program. Reviewing ARS CIP related incidents for systemic problems and opportunities for process improvements. Reviewing annual ARS self-certifications for evidence completeness.On a regular basis, reviewing and updating EDTI's position in EPCOR's cyber security framework documentation, and leading collaboration with SMEs across EDTI.Providing specialized technical level SME advice, guidance, and assistance as required, to teams within EDTI and EPCOR on ARS CIP compliance. Providing evidence for regulatory, security, and policy audits. Providing accurate and timely responses to audit information requests.Providing technical and business analysis, developing business cases and participating in regulatory filings related to cyber security initiatives. Assisting in the planning, development, and execution of training programs designed to ensure compliance with ARS CIP and related internal cyber security policies.Maintaining awareness of emerging utility industry compliance issues, through benchmarking and participation in appropriate forums/groups. Staying up to date on new versions of NERC and ARS standards and participating in industry consultation. Distributing relevant information to impacted SMEs and providing education as required. Developing and maintaining business unit KPIs for cyber security related metrics. Participating in or leading cross-functional teams to design and maintain dashboards to support EDTI's cyber security posture.Effectively and clearly communicating highly technical information both verbally and in writing to team members, management, executive, and others.

What's required to be successful

A degree in Cybersecurity, Computer Science, Information Technology or a related disciplineRelated disciplines: Engineering, business administration, management of information systems, etc.
5+ years of equivalent experience in IT cyber security or related area and/or 3+ years working specifically in a Critical Infrastructure Protection information security operations or consulting function2+ years of experience with ARS / NERC CIP regulatory requirementsWorking experience with cyber security frameworks (C2M2, NIST CSF, CIS)Experience performing assurance work (audits/reviews), and business risk assessmentsSecurity-related training/certifications are an asset (CISA, CISSP, CISM, CIRSC)Proficiency in business writing for the preparation of reports and presentationsEffective presentation skills, appropriate for senior or executive management levelsExperience managing and analyzing data from system event logs, SIEM logs, firewall rules, and baseline reporting softwareSecurity experience including threat identification, kill chain risk analysis, proactive defense, incident response, and development of mitigation strategies is an assetExperience with protection and control, automation, telecontrol and SCADA operational technologies is an assetStrong reporting and data analysis skillsetExperience with business and process analysis
Ã‚Â Other important facts about this job
Jurisdiction: ProfessionalHours of work: 80 hours biweeklyÃ‚Â Application deadline: July 18, 2022Ã‚Â EPCOR employees: please ensure that you are using your "@epcor.com" email address.Ã‚Â This position may be eligible for a $2,000 employee referral reward! Ensure you enter Employee Referral as the referral source when you are applying.Ã‚Â Ã‚Â Learn more about Working at EPCOR!Follow us on LinkedIn,Ã‚Â Twitter, GlassdoorÃ‚Â or Facebook!Ã‚Â #LI-TA2Ã‚Â Please note the following information:A requirement of working for EPCOR is that you are at least 18 years of age, successfully attained a high school diploma (GED, or equivalent level of secondary education) and legally entitled to work in Canada. (A copy of a valid work permit may be required.)If you are considered for the position, clearance on all applicable background checks (which may include criminal, identity, educational, and/or credit) and professional reference checks is required. Some EPCOR positions require an enhanced level of background assessment, which is dictated by law. These positions require advanced criminal record checks that must also be conducted from time to time after commencement of employment.A technical/practical assessment may be administered during the selection process and this exercise will be used as a part of the selection criterion.To meet the physical demands required of some positions, candidates must be in good physical condition and willing to work in all weather conditions. Clearance on pre-placement medical and drug and alcohol testing may be required.
Ã‚Â

For more information, visit EPCOR for Specialist, Security Policy & Audit