Make working for The City work for you.

Information Security Advisor - AMENDMENT

If you are committed to public service, enjoy collaborating with others, share our values and have a desire to learn and grow, join The City of Calgary. City employees deliver the services, run the programs and operate the facilities which make a difference in our community. We support work-life balance, promote physical and psychological safety, and offer competitive wages, pensions, and benefits. Together we make Calgary a great place to make a living, a great place to make a life.

The City is committed to fostering a respectful, inclusive and equitable workplace which is representative of the community we serve. We welcome those who have demonstrated a commitment to upholding the values of equity, diversity, inclusion, anti-racism and reconciliation. Applications are encouraged from members of groups that are historically disadvantaged and underrepresented. Accommodations are available during the hiring process, upon request.

As an Information Security Advisor, you will be responsible for supporting the strategic and tactical initiatives of the Information Security Compliance & Advisory team. You will also work closely with business units to develop, implement and promote an information security and risk-aware culture following an Enterprise Security Risk Management (ESRM) approach. Primary duties include:

- Perform risk assessments on technology projects, initiatives and infrastructure by working closely with interested parties to identify, classify, and mitigate cyber threats.
- Provide information security expertise and advice to Information Technology (IT), Operations Technology (OT), Internet of Things (IoT), other business units and associated projects.
- Define and implement security controls, architecture, and security testing of the Operational Technology based on asset criticality and risk assessments.
- Participate in vulnerability identification; manage the Vulnerability Management program and collaborate with interested parties on remediation plans and tasks.
- Research, develop and implement ICS security policies, standards, procedures, controls, frameworks and incident response plan and playbook identified as project deliverables.
- Partner with the ICS Program Manager to support and help monitor implementation and program sustainment.
- Advise system administrators on security tools such as Vulnerability Management, application systems, assets inventory, OTICS security zones architect.

Qualifications

- A completed 2-year Technology Diploma and at least 8 years of Information Security or related experience, OR;
- A degree in Information Technology, Computer Science or a related discipline and at least 4 years of Information Security or related experience.
- Equivalent combinations of experience and education may be considered.
- Expertise on assessing cyber security vulnerabilities, risks, threats and various control mechanisms to mitigate business risks particularly in OTISC environments is required.
- Experience in designing, architecting and implementing cyber security ICS frameworks such as NIST, ISO, NERC.
- One or more recognized Security certifications such as Certified Information Systems Security Professional (CISSP), Certification in Risk and Information Systems Control (CRISC), Global Industrial Cyber Security Professional (GICSP), or Global Information Assurance Certification (GIAC) is preferred.
- Experience performing security/threat assessment of Enterprise applications, Cloud-based services (IaaS, PaaS, SaaS, etc.), IT network, Industrial Control Systems (ICS), and Internet of Things (IoT) is an asset.
- Experience working in Operational Technology (OT), OT risk assessment and mitigation is an asset.
- An understanding of server platforms (for example: Linux, Windows), networking, security (Firewalls, IDS/IPS, SIEM, xDR, DMZ, Zero Trust, Purdue Model, proxy systems) and experience with UNIX and Windows Command Line Interface.
- Technical experience with OT Vulnerability Management and Endpoint Protection systems in large enterprise deployment.
- Knowledge of how malicious code operates, how technical vulnerabilities are exploited, and knowledge of cyber threats, defenses, motivations and techniques will also be considered an asset.
- Previous experience in Operational Technology and working in a municipal government and a broad knowledge of the types of services provided by a large municipality will be beneficial.
- Well-developed interpersonal and communication skills, organization and planning skills and the ability to effectively prioritize and work in a team setting.

Pre-employment Requirements

- A security clearance will be conducted.
- Successful applicants must provide proof of qualifications.

Union: Exempt	Business Unit: Corporate Security
Position Type: 1 Permanent	Location: 133 6 Avenue SE
Compensation: Level E $83,059 – 125,413 per annum	Days of Work: This position works a 5 day work week earning 1 day off in a 3 week cycle.
Hours of work: Standard 35 hour work week	Apply By: July 17, 2024
Audience: Internal/External	Job ID #: 310054
Amendment: Apply By Date	

Apply online at www.calgary.ca/careers