RPRA
Resource Productivity
& Recovery Authority

Security Specialist
Career Opportunity
March 2021

Are you passionate about protecting the environment? Do you go out of your way to reduce, reuse, and recycle? Do you envision a waste-free future?

If you answered yes to those questions, then we'd like to hear from you.

We are the Resource Productivity and Recovery Authority (the Authority) and our vision is a circular economy today for a waste-free tomorrow. Our mission is to support compliance with individual producer responsibility through education and enforcement to foster Ontario's circular economy, spur innovation, and protect the environment.

Our mandate from the Government of Ontario is to advance a circular economy by enforcing the requirements of the *Resource Recovery and Circular Economy Act, 2016* (RRCEA) and the *Waste Diversion Transition Act, 2016* (WDTA) and their related regulations.

We are looking for a talented and committed individual to join us as a **Security Specialist** to support the government's efforts to protect the environment and accelerate a new economy in which all waste is reused, recycled and reintegrated.

Security Specialist

The Security Specialist will manage and support the overall corporate Information Technology security landscape. This role will work with technology including but not limited to: Windows Server, Active Directory, VMWare, Exchange 2016 and Exchange Online, MS Office, One Drive, SharePoint, Amazon Connect, Sophos (or other) Firewall and Salesforce Service Cloud and Marketing Cloud. This also includes network and telecommunication systems as well as applications and systems which directly support the end user computing environment.

In addition to IT operations activities, this role will participate in technology research, budgeting, facilities security support, procurement, and deployment.

Practically speaking, you will:

Security Landscape

- Support the organization's security program and security operations
- Responsible for ensuring all information systems are secure
- Analyze IT specifications to assess security risks
- Participate in IT and Business initiatives promoting adherence to security policies and standards for security domains as follows:
    - Security risk management
    - Endpoint security
    - Perimeter defense
    - Vulnerability management
    - Vendor risk management

- Establish and maintain a security baseline for secure configuration of information assets
- Assist with the security reviews of networks, systems, hosted environments, and services
- Support incident response activities and triage involving collection of event data, detailed analysis of audit logs, and reporting
- Design and implement security measures and controls
- Act on privacy breaches and malware threats
- Security configuration management of hosts, network devices, and security appliances and technologies as follows:
    - SIEM (Security information and event management) rule creation and log analysis
    - Firewall rule configuration
    - Vulnerability scanning
    - OS security hardening
    - Network device hardening
    - Security appliance configuration
- Develop, implement and enforce security standards per company's information and security policies, controls and procedures
- Support system implementations, modifications and enhancements, identifying security gaps and preparing action plans to address
- Technical security documentation development
- Support regular patch upgrades and major technology upgrade initiatives, examining defensive system and provide reports on test results
- Conduct security audit activities and vulnerability assessments
- Assists in designing and developing security features for system architectures
- Design and conduct staff training on security policies, best practices and procedures

Facilities Security Support

- Assist CIO with the ongoing support of our overall facilities security including working with building and vendor staff on an as required basis to address RPRA needs

Budgeting

- Working with the CIO, assists in the development and management of the I&IT annual operating and capital budgets from a security point of view

Working at the Resource Productivity and Recovery Authority

This is a permanent full-time role working Monday-Friday from 9:00am-5:00pm, with flexibility as needed. Our highly attractive total compensation plan includes a competitive salary (commensurate with experience), health benefits, a defined contribution pension, personal days and three weeks of vacation to start.

During COVID-19, we work remotely and support flexible work schedules. Upon our return to the office, you'll need to be able to commute to our office. We are conveniently located in North York on the Yonge subway line at Sheppard Avenue.

We are a small team operating in an entrepreneurial environment. We are looking for team players who know what all hands-on deck means, can hit the ground running, and are ready to make the job their own. You'll have plenty of opportunities for growth, development, and mentorship as you learn from our talented team. Our hope for you is that you'll be able to fine-tune your skills and move upward in our organization.

You will be a part of a collaborative team doing ground-breaking and meaningful work with a critical environmental and economic mission.

Qualifications:

- Bachelor's Degree or equivalent expertise in Computer Science, Information Security Management or similar field
- Minimum of 5 years' experience working in information security
- Minimum of 5 years' experience implementing security controls in an enterprise environment.
- Must hold a current cybersecurity certification (i.e., GSEC, GCIH, GCCC, GDAT, GCWN, GPEN, OSCP)
- Experience implementing a security protocol to ensure a secure Office 365 environment with SaaS hosted Exchange, OneDrive and SharePoint
- Familiarity with a complex regulatory environment or public-sector entity an asset
- Agile methodology experience

Here are some things that will make you stand out:

- Sound knowledge and expertise in I&IT strategic and operational planning
- Experience in analysis, implementation and evaluation of I&IT security systems and their specifications
- Sound decision-making skills within the context of complex and sometimes conflicting priorities
- Ability to engage and sustain effective relationships with internal and external stakeholders
- Ability to foster a collaborative work environment that promotes and facilitates transparency and accountability
- Excellent problem-solving and consensus building skills
- Strong project management, organizational and time management skills
- Excellent analytical and evaluative skills
- Ability to meet deadlines, to conduct and direct research into I&IT security issues and products, and to take initiative in the development and completion of projects
- Outstanding verbal and written communications ability
- Knowledge of full systems development life cycle (SDLC) preferred
- Early identification of potential risks to budget and schedule developing and implementing appropriate mitigation strategies
- Demonstrated ability to thrive in a dynamic, fast-changing environment
- Comfortable with ambiguity, frequent change, or unpredictability
- Self-motivated and organized to manage multiple and competing priorities
- Known for being a team player ready to collaborate and pitch in where required
- Discretion and judgement in working with confidential information

How to Apply

We strive to build a team that reflects the diversity of the community we work in and encourage applications from traditionally underrepresented groups such as women, visible minorities, Indigenous peoples, people identifying as LGBTQ2SI, veterans and people with disabilities.

Please submit your CV and cover letter to:

careers@rpra.ca