JOB DESCRIPTION

Job Title: Cybersecurity Specialist, IT **Position Number:** 90-06

Incumbent: Vacant **Effective Date:** January 2025

Status: Permanent **Pay Level** 10 **Bargaining Unit:** X **Yes** __ **No**

Supervisor's Title: Manager, IT **Department:** Information Technology

SUMMARY

Reporting to the IT Manager, the Cybersecurity Specialist will strengthen the IT security posture of our organization within the utility sector. The successful candidate will be responsible for implementing and maintaining cybersecurity strategies aligned with the NIST Cybersecurity Framework (CSF) 2.0, managing IT infrastructure security, conducting Security Threat Risk Assessments (STRA), and supporting business continuity and incident response planning. This position requires a proactive approach to identifying and mitigating risks and the ability to work in a dynamic, fast-paced environment. Flexibility and attention to detail are essential. All work shall be carried out and properly documented in accordance with Yukon Energy's policies, guidelines, and procedures.

DESCRIPTION

Cybersecurity Operations:

- Implement and manage IT security measures, including access controls, firewalls, endpoint protection, and monitoring tools.
- Conduct real-time analysis of security alerts and coordinate responses to mitigate threats.
- Perform vulnerability assessments and oversee patch management processes for IT systems.

Compliance and Standards:

- Ensure IT security operations align with NIST CSF 2.0 and CIS/IEC 62443 standards.
- Prepare documentation and evidence for audits and assessments related to regulatory and industry standards.
- Monitor compliance with corporate policies, standards, and risk management strategies.

Incident Response and Tabletop Exercises:

- Develop and refine incident response plans (IRPs) for IT environments.
- Coordinate and lead tabletop exercises to simulate cyber incidents, ensuring preparedness across IT and operational teams.
- Analyze post-incident reviews to identify improvements in IT security protocols.

Business Continuity, Backup Reviews, and Disaster Recovery:

- Collaborate with IT and business units to maintain and update Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs).
- Conduct regular backup reviews to ensure critical data and systems can be restored in a timely and secure manner.
- Test IT systems' resilience to ensure alignment with organizational recovery objectives.
- Provide guidance on IT risk assessments and support the continuity of critical business functions.

Security Threat Risk Assessments (STRA) and Reviews:

- Perform detailed Security Threat Risk Assessments (STRA) to identify, analyze, and mitigate risks associated with IT systems and applications.
- Review architecture designs and proposed changes to IT systems to ensure security considerations are addressed.
- Provide recommendations for secure implementation of new technologies and systems.

Cybersecurity Point of Contact:

- Act as the primary cybersecurity liaison for IT infrastructure projects, ensuring that security requirements are integrated into project plans and implementations.
- Collaborate with internal teams and external partners to address cybersecurity concerns, provide guidance, and mitigate risks.
- Represent the organization in discussions with vendors, auditors, and regulators, offering expert input on IT security matters.

EDUCATION AND EXPERIENCE

- Bachelor’s degree in Cybersecurity, Information Technology, Computer Science, or related field. Certifications such as CISSP, CISM, CompTIA Security+, or Certified Ethical Hacker (CEH) are highly desirable.
- 3-5 years of IT security experience, preferably in utilities or critical infrastructure sectors.
- Hands-on experience with compliance frameworks like NIST CSF 2.0 and CIS/IEC 62443.
- Familiarity with IT systems, including cloud platforms (e.g., AWS, Azure), Windows/Linux servers, and Active Directory.

KNOWLEDGE AND SKILLS

- Experience with tools and platforms such as Cisco, Check Point, and NetScaler
- Capability to evaluate risks and recommend actionable mitigation strategies.
- Hands-on experience in Incident Response, BCP/DR testing and simulation.
- Understanding of securing cloud platforms.
- Strong understanding of network security, including firewalls, VPNs, and intrusion detection/prevention systems (IDS/IPS).

- Strong understanding of network protocols (TCP/IP, OSI model), routing, switching, firewalls, VPNs, and network security architectures.
- Experience with configuring and maintaining secure network environments.
- Strong understanding of threat landscapes, attack vectors, and mitigation strategies.
- Knowledge of securing IT infrastructure, including servers, databases, and cloud systems.
- Proficiency in endpoint protection platforms, antivirus, and vulnerability management tools.
- Expertise in performing STRA and creating actionable mitigation strategies.
- Knowledge of data loss prevention (DLP) technologies and encryption protocols.
- Exceptional problem-solving and analytical skills.
- Effective written and verbal communication.
- Detail-oriented with the ability to prioritize and manage multiple tasks.
- Evaluating complex problems systematically to identify root causes and solutions.
- Drafting policies, reports, and incident summaries clearly and concisely.

WORKING CONDITIONS

This role primarily involves work in an office setting. Candidates must be available for periodic on-call duties in response to cybersecurity incidents.

CONDITIONS OF EMPLOYMENT

Employment is conditional upon the successful completion of a criminal record check, which will only be conducted after a conditional offer of employment has been made. This requirement reflects the sensitive nature of the position.

The candidate will also be required to provide proof of qualifications or certifications applicable to the role.