CYBERSECURITY SPECIALIST – DATA PROTECTION

Department: Information Technology & Telecom
Unit: 5210
Level: 6, Non-Exempt

Supervisor's Title: Cybersecurity Manager
Supervises: No Staff

Purpose
The Cybersecurity Specialist – Data Protection is responsible for safeguarding Massport's data assets by implementing robust protection, classification, and compliance measures across cloud and on-premises environments. The Specialist leads efforts in data security, mobile endpoint protection, system administration, and cross-functional collaboration to ensure secure architectures, minimize risk, and continuously improve cybersecurity practices in alignment with industry standards and organizational goals.

Our Information Technology (IT) Department's mission is to provide innovative, robust, and secure information and telecommunication systems for employees and members of the public who use Massport's facilities and systems. We strive to provide efficient and accessible technology to enable Massport to successfully meet its business goals and promote local and regional economic prosperity. We are a service-based organization that works collaboratively across departments to provide technological leadership, resources, technology education and tools in support of the Authority. The Cybersecurity Team is responsible for the design, implementation, and monitoring of all technology-based security services across the enterprise environment.

ESSENTIAL JOB RESPONSIBILITIES

Data Protection and Classification

- Identify, document and secure all repositories containing Massport data, including those stored in cloud environments and on-premises systems.
- Develop and maintain an up-to-date inventory of all structured and unstructured data assets, including ownership, sensitivity, and storage locations.
- Implement and manage a data classification framework to categorize data based on sensitivity (e.g., public, internal, confidential, restricted).
- Lead efforts to evaluate and secure AI, BI, and cloud-based data platforms to ensure alignment with enterprise security standards. Implement safeguards for sensitive data through access controls, encryption, data classification, and continuous monitoring. Collaborate with cross-functional teams to design secure architectures and enforce governance across cloud environments where enterprise data is stored and processed.

- Research and evaluate industry best practices for data protection to ensure the organization's strategies remain effective and up to date.
- Implement and manage security technologies to minimize the risk of data loss.
- Collaborate with data owners and custodians to ensure proper handling, security, and compliance for all organizational data assets.
- Track and analyze data flows across the organization to identify unauthorized transfers or access to sensitive information.
- Draft and update data security policies and guidelines to ensure the protection of organizational data.

Mobile Endpoint Security

- Ensure that all devices, services, and users meet defined security controls and compliance requirements prior to accessing data across all classification levels.
- Strengthen mobile endpoint security through policy configuration, device monitoring, and remediation of non-compliant assets. Collaborate with all business units to maintain a secure mobile ecosystem that supports secure access to enterprise resources.

System Administration and Installation

- Oversee, support, and administer additional security systems as delegated.
- Create, verify, and/or maintain documentation of assigned information systems.
- Ensure security and system integrity of assigned information systems.
- Assist with troubleshooting of all security related software and systems.
- Assist with the physical installation of cybersecurity hardware, such as firewalls, servers and appliances.

Continuous Improvement and Cross-Functional Collaboration

- Ensure Massport Help Desk and support staff are properly trained to troubleshoot and assist users impacted by data protection security controls.
- Participate in new product research and development of emerging security technologies that may be used to replace, augment or layer into the existing Massport IT topology.
- Work with all other Massport IT teams to securely implement new systems and improve security of existing systems.
- Attend meetings with all business units and outside contractors to provide advice on implementation of new systems and cybersecurity best practices.

Perform other tasks as necessary.

JOB REQUIREMENTS AND QUALIFICATIONS

<u>Education</u>

Bachelor's degree in computer science, cyber certifications, or equivalent professional work experience preferred.

Experience
1-3 years of hands-on experience with cybersecurity systems or enterprise computer systems administration.

SKILLS AND COMPETENCIES

- Strong understanding of security principles and best practices, with emphasis on data protection methodologies and regulatory compliance.
- Ability to triage, prioritize, and respond to cybersecurity alerts and investigations effectively.
- Working knowledge of enterprise hardware including workstations, servers, and laptops, with a focus on secure configuration and management.
- Proficient in modern operating systems (Windows Desktop, Windows Server, Linux), including security hardening and patch management.
- Skilled in troubleshooting hardware, software, and network issues with a security-first approach.
- Experience administering Microsoft 365 and managing cloud environments (Azure/AWS), with attention to identity, access, and data security.
- Hands-on experience with Data Loss Prevention (DLP) platforms, particularly Microsoft Purview, for securing sensitive data.
- Familiarity with enterprise-grade security monitoring and management solutions (e.g., SIEM, EDR, XDR) to support threat detection and response.

WORK SCHEDULE AND OTHER REQUIREMENTS

- This position is based at Massport's Logan Office Center and requires flexibility to meet the dynamic needs of the department.
- Ability to work 37.5 hours per week.
- Ability to respond to emergency calls after normal business hours, 7 days per week, 24 hours per day and 365 days per year.
- Ability to pass Massport's pre-employment-controlled substance test and background checks.
- Current and valid driver's license.