MAINE MARITIME ACADEMY

A College of Engineering, Management, Science, and Transportation

INFORMATION SYSTEMS SECURITY OFFICER

POSITION OVERVIEW

Reporting to the CTO, the Information Systems Security Officer (ISSO) is responsible for developing and implementing security measures to protect Academy computer systems, networks, and digital information. The ISSO will work closely with the IT team and Academy management to identify potential security vulnerabilities, analyze security risks, and ensure compliance with industry regulations. The ISSO has a solid understanding of information security principles, excellent problem-solving skills, and the ability to communicate effectively with both technical and non-technical personnel. This position is a full-time, 12-month, benefited SSP staff position.

DUTIES

- Develop and maintain a comprehensive information security program to safeguard the organization's data, systems, and networks.
- Designs, maintains, and executes vulnerability testing processes and security breach mitigation tactics.
- Assists in the selection of appropriate controls, control objectives, and activities to achieve policy goals and regulatory compliance.
- Designs, configures, implements, and maintains all security platforms and associated software including routers, switches, firewall, VPNs, WAF, NIDPS, SIEM, anti-SPAM, anti-virus, anti-malware, cryptology systems and MDM.
- Designs, reviews, and continuously assesses firewall, intrusion detection/prevention, SIEM, VPN, SSL, application control, anti-virus and other network component policies and underlying systems.
- Performs security reconnaissance on assets, gathering intelligence to identify and respond to potential security threats and vulnerabilities of

moderate organizational risk and complexity, ensuring appropriate threat mitigation procedures are followed.

- Responsible for major security platform upgrades and changes.
- Coordinates and oversees third party penetration testing and security audits.
- Coordinate incident response activities, investigate security breaches, and provide recommendations for incident mitigation.
- Maintains up to date baselines for secure configuration and operation of all systems infrastructure.
- Performs security analysis of new and existing security applications and operating systems including hosted solutions. Applies standards to new installations before they transition from development to production environments.
- Performs regular analysis of all infrastructure systems to assess security vulnerabilities and needs.
- Coordinates and oversees log analysis for external monitoring services provider.
- Monitors data security systems to identify security events and leads event response efforts.
- Interfaces with external vendors to assess network access requests and ensure that they meet adopted standards and best practices.
- Stay up to date with the latest information security trends, technologies, and best practices to ensure continuous improvement of the organization's security posture.
- Educate and train employees on best practices for information security, data privacy, and incident response.
- Collaborate with internal and external stakeholders to address security concerns, implement security standards, and ensure compliance with regulatory requirements. Responsible for all security related training for the institution.
- Collaborates with CTO to create policies, procedures and best practices.
- Other duties as assigned.

SKILLS

- Excellent customer service skills, and the ability to work well with both internal (Academy) customers as well as external entities.
- Ability to keep up to date with quickly changing field of network and information system security.
- Knowledgeable with industry standards and best practices for network and data security.
- Strong organizational and time management skills.
- Exceptional troubleshooting ability required to solve non-routine, complex problems as they arise.
- Computer hardware and software skills are required.
- Ability to troubleshoot and repair hardware and software.
- Critical thinking skills.
- Analytical and technical aptitude to focus on identification and resolution of root causes of issues; holistic approach.
- Ability to work in a team oriented, collaborative environment is required.

QUALIFICATIONS

- 5 years of prior experience in a complex computing environment is required.
- Bachelor's degree in Computer Science, Information Technology, or in related field is highly desired.
- CISSP certification or ability to obtain within 12 months of hire is required.
- CISM, Security +, Network+, or other additional security and network certifications are preferred.
- In-depth knowledge of information security principles, methodologies, and best practices.
- Familiarity with industry standards and regulations (e.g., ISO 27001, NIST, HIPAA, etc.).
- Experience in conducting risk assessments and implementing security controls.
- Proficiency in using security tools and technologies, such as firewalls, intrusion detection systems, SIEM, and vulnerability management tools.

- Strong analytical and problem-solving skills to identify security gaps and develop effective mitigation strategies.
- Strong written and oral communications skills are required.
- Ability to work independently and collaborate with cross-functional teams to achieve common security goals.
- Knowledge of incident response procedures and familiarity with forensic tools is a plus.

WORKING CONDITIONS

- Environment can be stressful, competing projects and demands frequent bending and twisting in awkward positions
- Frequent contact with students, parents and external entities
- Some lifting of moderately heavy equipment for various reasons
- Occasional weekend and evening work required

Maine Maritime Academy Position Factor Evaluation			
	Job Title: Information Systems Security Officer	Job Code:	
	Wage Grade: 25	Total Points: 546	
	Factor	Degree	Points
1	Knowledge and Skill	8	288
2	Effort		
	A. Mental and Visual Effort	5	40
	B. Physical Effort	3	30
3	Responsibility for Cost Control	5	40
4	Responsibility for Others		
	A. Injury to Others	2	16
	B. Supervisory Responsibility	3	24
	C. Sensitive Information and Records	5	40
5	Working Conditions	2	20
6	Responsibility for External and Internal Relations	6	48
	Date of last reclassification: 02-13-2025		