SLASPA
SAINT LUCIA AIR AND SEA PORTS AUTHORITY

JOB DESCRIPTION

POSITION IDENTIFICATION		FUNCTIONAL RELATIONSHIPS	
Job Title:	**IT Security Specialist**	**Direct Reports:**	
Reports to:	Systems Administrator	**Internal Contacts:**	SLASPA Employees
Department:	Information Systems	**External Contacts:**	SLASPA Stakeholders
Classification	Grade 5	**Reviewed**	June 2026

JOB SUMMARY:

The IT Security Specialist is responsible for protecting the company's information systems and networks from cyber threats. This role involves implementing and managing security measures, conducting risk assessments, monitoring network traffic, and responding to security breaches. The IT Security Specialist collaborates with other IT professionals and departments to ensure the security and integrity of the company's data and systems.

DUTIES AND RESPONSIBILITIES

Security Operations

1. Network Traffic Monitoring: Continuously monitor network traffic using various tools to detect unusual activity, potential threats, and security breaches.
2. Security Tools Management: Installs, configures and maintains security tools and technologies including but not limited to endpoint security, access control, firewalls, encryption, network security and intrusion detection/prevention.
3. Vulnerability Assessments: Conducts regular vulnerability assessments to identify security weaknesses and potential threats within the network and systems. Develop strategies to mitigate these vulnerabilities.
4. Patch Management: Liaises with relevant IT personnel to ensure all systems and applications are up to date with the latest patches and security updates to protect against vulnerabilities.

Incident Response

5. Incident Investigation: Quickly and efficiently investigate security breaches, anomalies, and incidents to determine their origin, impact, and the best course of action for resolution.
6. Response Plan Execution: Develops, documents, and executes incident response plans to contain and remediate security incidents. Coordinates with internal teams to implement corrective actions.
7. Reporting and Documentation: Maintains detailed records of security incidents, including root cause analysis, incident response actions, and lessons learned. Prepare reports for management and stakeholders.
8. Coordination with External Entities: Works with external cybersecurity agencies, law enforcement, and other organizations as necessary to address significant security incidents.

Policy and Compliance

9. Policy Development: Develops, reviews, and updates security policies, standards, and procedures to ensure they align with industry best practices and regulatory requirements.
10. Compliance Assurance: Ensures the organization complies with relevant security standards, adopted policies and regulations such as GDPR among others. Conduct regular compliance audits and assessments.

Education and Training

11. Employee Training: Develops and delivers cybersecurity training programs to educate employees on security best practices, phishing awareness, and safe online behaviors.
12. Security Awareness: Promotes a culture of security awareness within the organization through regular communications, workshops, and awareness campaigns.
13. Resource Provision: Provides resources, guidelines, and tools to help employees understand and adhere to security policies and procedures

Research and Development

14. Threat Intelligence: Stay current on the latest cybersecurity threats, vulnerabilities, and trends by conducting ongoing research and participating in professional cybersecurity communities.
15. Security Innovation: Research and recommend new security technologies and methodologies to improve the organization's security posture. Evaluate and implement new security solutions.
16. Continuous Improvement: Continuously assess the effectiveness of existing security measures and recommend improvements. Stay informed about the latest security tools and techniques.

17. Performs any other related duties as assigned by the Supervisor from time to time

QUALIFICATIONS AND EXPERIENCE

- Bachelor's degree in computer science, Information Technology, Cybersecurity, or a related field plus two (2) years experience in information security or related field.
- Proven experience with security technologies and practices.
- Professional certifications such as CISSP, CISM, CCSA, Certified Ethical Hacker, or CompTIA Security+ are highly desirable.

KNOWLEDGE, SKILLS AND ABILITIES

- Demonstrates a high level of confidentiality, competency and professionalism at all times
- Strong communication and interpersonal skills.
- Excellent time management and organizational skills.
- Excellent writing skills.
- Active listening skills.
- Function within a team environment.
- Ability to be flexible with work assignments.
- Ability to use one's initiative and be proactive.

- Strong knowledge of network protocols and cybersecurity principles.
- Proficiency in security tools (e.g., SIEM, IDS/IPS, DLP).
- Excellent analytical and problem-solving skills.
- Ability to work under pressure and handle multiple tasks simultaneously.

SIGNATURE

I confirm that the requirements of this job description were discussed with me and I understand what is expected of me.

Employee's Name : _____

Employee's Signature : _____

Date : _____