



CIVIL SERVICE OF JAMAICA
JOB DESCRIPTION AND SPECIFICATION
MINISTRY OF ENERGY, TRANSPORT AND TELECOMMUNICATIONS (METT)

JOB TITLE:	Cyber Security Specialist
JOB GRADE:	MIS/IT 7
POST NUMBER:	58530
DIVISION:	Corporate Services Division
BRANCH/UNIT:	Information Systems Branch
REPORTS TO:	Director, Management Information Systems
MANAGES:	Incident Responder

This document will be used as a management tool and specifically will enable the classification of positions and the evaluation of the performance of the post incumbent.

This document is validated as an accurate and true description of the job as signified below:

Employee

Date

Manager/Supervisor

Date

Head of Department/Division

Date

Date received in Human Resource Division

Date Created/revised

JOB PURPOSE

Under the strategic direction of the Senior Director, Information, Communications and Technology, the Cybersecurity Specialist leads the Ministry's cybersecurity programme, ensuring the protection of all digital assets, systems, and infrastructure. The role is responsible for policy development, strategic planning, governance, risk management, and national cybersecurity coordination, ensuring alignment with legislative requirements such as the Data Protection Act and international best practices.

KEY OUTPUTS

- Enterprise-wide cybersecurity strategy implemented and continuously improved
- Full compliance with national cybersecurity and data protection regulations
- Mature incident response and threat intelligence capability
- Cyber risk posture continuously assessed and reduced
- Quarterly cybersecurity reports to Senior Leadership
- Effective coordination with national cybersecurity bodies (e.g., JaCIRT, NSOC, MOCA)
- Security awareness culture embedded across the Ministry

KEY RESPONSIBILITY AREAS

Management / Administrative Responsibilities

- Provides strategic leadership and direction for cybersecurity
- Develops and oversees cybersecurity policies, frameworks, and standards
- Leads cybersecurity risk management and governance processes
- Advises executive leadership on cyber risks and mitigation strategies
- Represents the Ministry at national and international cybersecurity forums
- Oversees budget planning and cybersecurity investments

Technical / Professional Responsibilities

- Oversees security architecture, engineering, and incident response functions
- Ensures implementation of enterprise security controls and monitoring systems
- Directs incident response, investigations, and reporting
- Oversees vulnerability management and threat intelligence programs
- Ensures secure system design and compliance with standards
- Evaluates emerging threats and technologies

Human Resource Management Responsibilities

- Provides leadership, guidance, and supervision to direct reports
- Monitors and evaluates staff performance and conducts performance appraisals
- Recommends and supports recruitment, training, and development of staff
- Promotes a culture of accountability, teamwork, and high performance
- Ensures staff are adequately resourced to perform their functions effectively
- Builds institutional cybersecurity capacity
- Recommends leave, disciplinary action, and staffing arrangements as required

PERFORMANCE STANDARD

- Cybersecurity strategy is developed, implemented, and periodically reviewed in alignment with organizational objectives.
- Policies, standards, and procedures are established, communicated, and updated within required timeframes.
- All applicable cybersecurity and data protection requirements are complied with, and audit issues are resolved within stipulated timelines.
- Security incidents are promptly detected, effectively managed, and reported accurately within established timelines.
- Cybersecurity risks are identified, assessed, and mitigated in a timely and structured manner.
- Security controls are implemented and monitored to safeguard systems and data, and vulnerabilities are addressed within defined timeframes.
- Reports are accurate, clear, and submitted within stipulated timelines.
- Effective collaboration is maintained with relevant stakeholders and national cybersecurity bodies, with information shared as required.
- Security awareness activities are implemented and contribute to improved staff compliance with security practices.

INTERNAL AND EXTERNAL CONTACTS:

<i>Internal</i>	<i>Nature of Relationship</i>
Director, Management Information Systems	Receive directives and guidance
Divisional heads, managers and supervisors	Provide and receive information

Enterprise Risk Management	Align on risk assessments, controls, support compliance activities.
Internal Audit Unit	Align on risk assessments, controls, and audit findings; support compliance activities
General Staff	Collaboration and sharing of information Training in cybersecurity awareness

<i>External</i>	<i>Nature of Relationship</i>
Portfolio entities	Provide Report on identified vulnerabilities
Jamaica Cyber Incident Response Team	Report incidents, share threat intelligence, and coordinate national response activities.
Office of the Information Commissioner Jamaica	Ensure compliance with the Data Protection Act and manage breach notifications.
Vendors / Service Providers	Ensure delivery of secure solutions and compliance with contractual security requirements.

REQUIRED COMPETENCIES

Core	Level	Functional	Level
Oral communication	3	Information Technology Security and Risk Management	4
Written communication	3	ICT Corporate Governance	3
Customer and quality focus	4	ICT Project Management	4
Team work and cooperation	4	Information Technology & Strategic Sourcing	3
Interpersonal skills	4	Analytical thinking	4
Compliance	4	Goal/result oriented	3
Integrity	4	Managing external relationships	4
Leadership	3	Problem solving and decision making	4
Initiative	4		
Planning and organizing	3		
Adaptability	3		

MINIMUM REQUIRED EDUCATION AND EXPERIENCE

- Bachelor's Degree in Cybersecurity, IT, or related field (Master's preferred)
- Minimum 7–10 years' experience, with at least 3 years in leadership
- Certifications: CISSP, CISM, C|EH or equivalent (required)

SPECIAL CONDITIONS ASSOCIATED WITH THE JOB

- Normal office conditions
- May be required to work beyond normal working hours;