



NATIONAL ENVIRONMENT AND PLANNING AGENCY

JOB DESCRIPTION AND SPECIFICATION

JOB TITLE:	ICT Security Officer
JOB GRADE:	Level 7
POST NUMBER:	
DIVISION:	Corporate Management
BRANCH:	Information & Communications Technology
REPORTS TO:	Manager – ICT Security
MANAGES:	N/A

This document is used as a management tool and specifically to 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

Strategic Objectives of the Division/Branch:

The Corporate Management Division provides a portfolio of organization support functions to enable efficient operations of the Agency in executing its mandate and the achievement of its objectives. The Division comprises the following Branches:

Finance & Accounts Branch: is responsible for managing the financial affairs of the Agency establishing and maintaining sound financial controls, accounting systems and procedures in keeping with standard accounting principles and practices and GoJs standards and requirements.

Public Education and Corporate Communication Branch is responsible for providing public education and consultation support services to the divisions and branches as well as to coordinate the Agency's public relations programmes.

Information & Communications Technology Branch: is responsible for the ongoing operations and technical support of the agency's technology infrastructure to support operational management and delivery of its services.

Facilities Management and Operations Branch: provides property, security, transport and maintenance management; office services management; and records management services.

Public Procurement Branch: provides procurement management services and administers procurements.

Job Purpose:

Under the management and direction of the Manager – ICT Security, the ICT Security Officer is responsible for supporting the monitoring and evaluation of the agency's ICT security management function in furtherance of the early detection of breaches and system vulnerabilities.

Key Outputs:

- ICT Security processes documented and maintained
- ICT Security infractions and violations monitored and analysed
- ICT Breaches investigated and reported
- Annual/Quarterly/Monthly/Periodic Reports prepared
- Technical advice and interpretation provided
- Individual Work Plan developed

Key Responsibility Areas:

Management Responsibilities

- Develops Individual Work Plans based on alignment to the overall plan for

the section;

- Participates in meetings, seminars, workshops and conferences as required;
- Prepares reports and programme documents as required;
- Maintains customer service principles, standards and measurements.

Technical/ Professional Responsibilities

- Participates in the development, implementation and maintenance of policies, procedures for network and security administration;
- Supports major cross-section of networking systems (e.g., remote access systems architecture, network core, building and departmental networks, wide area connectivity);
- Contributes to the design and deployment of the organisation's LANs, WANs, and wireless networks, including servers, routers, switches, UPSs, and other hardware;
- Assists with the design, implementation, and supports firewalls, site-to-site VPNs, and remote-access VPNs Conduct research on network products, services, protocols, and standards to remain abreast of developments in the networking industry;
- Interacts with vendors, outsourcers, and contractors to secure network products and services;
- Configures networks to ensure their smooth and reliable operation for fulfilling business objectives and processes;
- Monitors network performance and troubleshoots problem areas as required;
- Creates and maintains documentation as it relates to network configuration, network mapping, processes, and service records;
- Provides assistance to other ICT teams in troubleshooting problems relating to products/solutions;
- Ensures network connectivity and security of all servers, workstations, telephony equipment, fax machines, and other network appliances;
- Practices network asset management, including maintenance of network component inventory and related documentation and technical specifications information;
- Monitors and analyses systems for ICT Security infractions and violations;
- Documents and reports the results of questionable user and system activity for information security inquiries;
- Performs server and security audits, and system backups and recovery;
- Participates in managing all network security solutions;
- Collects and analyses operational data to identify emerging trends and log problem records to assist with problem resolution and increased network availability;
- Monitors and reports on the performance of network, system and application security solutions to highlight areas of non-compliance and inform the development of improved practices and processes;
- Manages the allocation of access privileges of users to ensure appropriate security settings are applied in accordance with organisation policies and application owner-defined parameters;
- Assists with security breach investigations to guide the refinement of information security policies and practices;
- Keeps abreast of changes and new developments in ICT Security and provides evidence-based recommendations.
- Keeps abreast of trends and developments in ICT and initiates/recommends

their use where necessary to improve the work of the agency.

Human Resource Responsibilities

- Contributes to and maintains a system that fosters a culture of teamwork, employee empowerment and commitment to the Division's and organization's goals;
- Assists with the preparation and conducts presentations on role of Division/Unit for the Orientation and Onboarding programme.
- Demonstrates and upholds the Agency's core values in personal and professional behaviours to minimize reputational risks and maintain the corporate image of the Agency.

Other Responsibilities

- The incumbent may, from time to time be assigned duties not specifically outlined within the job description but are, however within the capacity, qualifications and experience normally expected from a person occupying this position.

Authority

- The position incumbent is authorized to:
 - Recommends ICT Network and Security strategies and programmes;
 - Investigates ICT Security breaches.

Performance Standards:

- ICT Security processes documented and maintained in accordance with relevant standards and timeframes;
- Information Security infractions and violations monitored and analysed in accordance with established procedures agreed timeframes;
- ICT Breaches investigated and reported in accordance with established standards, SLAs and timeframes;
- Technical advice and recommendations provided are sound and supported by qualitative/quantitative data;
- Annual/Quarterly/Monthly performance reports are prepared in accordance with agreed format, are accurate and submitted on time;
- Individual Work Plans developed in conformity to established standards and within agreed timeframes;
- Confidentiality, integrity and professionalism displayed in the delivery of duties and interaction with staff.

Internal and External Contacts:

(i) Internal

Contact (Title)	Purpose of Communication/Contact
Director, ICT Manager, ICT Security	<ul style="list-style-type: none">• Provide advice and contribute to decision making;• Identify emerging issues/risks and their implications, and propose solutions;• Receive guidance and provide regular updates on key ICT Security Management

Contact (Title)	Purpose of Communication/Contact
	issues and priorities.
Senior Executives/Management in Divisions	<ul style="list-style-type: none"> • Develop and maintain effective working relationships • Collaborate, exchange information, provide strategic ICT Security Management advice, support and feedback
General Staff	<ul style="list-style-type: none"> • Develop and maintain effective relationships • Provide expert advice and exchange information

(ii) External Contact (required for the achievement of the position's objectives)

Contact (Title)	Purpose of Communication/Contact
MDAs	<ul style="list-style-type: none"> • Develop and maintain effective relationships; • Provides expert advice on ICT Security Management matters; and exchange information; • Liaise on key ICT Infrastructure Management issues
Ministry of Science, Energy & Telecommunications & Transport Office of the Prime Minister -ICT Authority	<ul style="list-style-type: none"> • Develop and maintain effective relationships; • Receive expert advice; and provide and exchange information; • Liaise on key ICT Security Management issues.
Professional Affiliations	<ul style="list-style-type: none"> • Provides expert advice and exchange information; • Identify innovation and new opportunities for the Association.
Contractors, suppliers and providers of services	<ul style="list-style-type: none"> • Monitors TOR for goods and services and related interventions; • Exchange of information.
General Public	<ul style="list-style-type: none"> • Collaborate on matters, exchange information, provide advice and seek feedback

Working Conditions

- Work will be conducted in an office outfitted with standard office equipment and specialized software.
- The environment is fast paced with on-going interactions with critical stakeholders and meeting tight deadlines which will result in high degrees of pressure, on occasions.
- Will be exposed to dust, dirt and confined spaces in performing infrastructure installation and maintenance activities;
- Will be required to endure the following physical demands: occasional lifting, carrying, pushing, and/or pulling; frequent climbing and balancing; some stooping, kneeling, crouching, and/or crawling; and significant fine finger

- dexterity;
- Will be required to travel locally to perform ICT infrastructure and security functions at outstations and to attend conferences, seminars and meetings.

Required Competencies:

- Working knowledge of LAN, WAN, and WLAN design and implementation.
- Working Knowledge of network capacity planning, network security principles, and general network management best practices
- Working technical knowledge of current network hardware, protocols, and Internet standards, including routers, switches, firewalls, remote access, DNS, VLAN, DSL, and Ethernet
- Good hardware troubleshooting experience and network monitoring and analysis software
- Good Knowledge about testing tools and procedures for voice and data circuits.
- Sound knowledge in defining organisational information security requirements
- Ability to identify and analyse information security risks
- Sound knowledge of user access control system to prevent unauthorized access, modification, manipulation etc.
- Demonstrates sound personal and professional integrity, reflecting high ethical and moral values
- Good Knowledge of GOJ ICT systems (existing and emerging);
- Good verbal and written communication skills, with the ability to deliver presentation with tact, clarity, enthusiasm and accuracy to widely varied audiences;
- A high level of initiative and self-motivation;
- Demonstrated interpersonal and negotiation skills.

Minimum Required Education and Experience

- Bachelor's degree in Software Design, Computing, Computer Science, ICT, Management Information Systems, Computer Engineering, or a related discipline;
- Three (3) years related experience in an ICT Security/Protection role.

OR

- Certified Information Security Manager (CISM) certification or related ICT security certification;
- Three (3) years related experience in an ICT Security/Protection role.

OR

- NVQJ Level 5 in Software Design, Computing, Computer Science, ICT, Management Information Systems, Computer Engineering, or a related discipline;
- Three (3) years related experience in an ICT Security/Protection role