NATIONAL ENVIRONMENT AND PLANNING AGENCY

JOB DESCRIPTION AND SPECIFICATION

JOB TITLE:	**Manager – ICT Security**
JOB GRADE:	Level 8
POST NUMBER:	338297
DIVISION:	Corporate Management
BRANCH:	Information & Communications Technology
REPORTS TO:	Director ICT
MANAGES:	ICT Security Officer

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:

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 leadership and direction of the Director – ICT, the Manager, ICT Security is chiefly answerable for leading the development, implementation and monitoring of ICT Security strategy, frameworks, policies and guidelines ensuring that the Agency successfully manages its compliance and obligations under the GOJ ICT Policies, Standards and Guidelines 2018.

Key Outputs:

- ICT Security risks mitigated
- Cyber security strategies managed
- ICT Infrastructure and Applications Audited
- ICT Security breaches reported and investigated
- Technical advice and interpretation provided
- Annual/Quarterly/Monthly performance reports prepared
- Individual work plans developed
- Staff coached and appraisals conducted

Key Responsibility Areas:

Management Responsibilities

- Manages the development of the Section's Corporate/Operational Plans, Budget and Individual Work Plans;
- Supervises preparation of reports to Director - ICT, CEO, Senior Executives and other relevant stakeholders;
- Represents Director - ICT at meetings, conferences, workshops and seminars;
- Prepares reports and project documents as required;
- Prepares and delivers ICT Security presentations as needed;

- Supports and maintains customer service principles, standards and measurements.

Technical/ Professional Responsibilities

- Assists the Director, ICT in the development and implementation of the ICT strategy, plans and policies as a senior staff of the ICT team;
- In partnership with the Manager – ICT Infrastructure & Technical Support designs, implements, and supports firewalls, site-to-site VPNs, and remote-access VPNs;
- Performs network monitoring and analysis, performance tuning, troubleshooting and escalating issues, including proactive problem resolution and complex problem analysis as necessary;
- Manages the design of mechanisms to reduce operational risk and improve availability of the network by ensuring network access, monitoring, control, evaluation and documentation practices are maintained and adhered to;
- Develops, maintains and performs operational procedures and ensure operational tasks are performed reliably and consistently to reduce the risk of unplanned outages;
- Evaluates new network hardware and software solutions for security threats and monitors the market for emerging technologies;
- Plans and implements backup storage and protection for the organisation's ICT landscape;
- Manages the development and implementation of cyber security strategy, framework, policies and guidelines, proactively assessing the current security posture for potential weaknesses and defensive gaps in order to ensure cyber safety and ensuring architectural principles are applied during design to reduce risk;
- Guides rigorous risk assessments to manage, rate and monitor risks related to cyber security, reviewing and updating these risks on a regular basis in order to actively promote a positive risk and compliance culture within the agency;
- Acts as the escalation/resolution point for sensitive/critical security incidents/alerts, which may require a flexible and adaptable approach to working hours and working arrangements to ensure an effective response and resolution of the security issue;
- Establishes procedures that facilitate the conducting of post-resumption reviews;
- Schedules workload and batches ICT operational job packages for ICT Security Officer(s);
- 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;
- Manages security breach investigations to guide the refinement of information security policies and practices;
- Manages the periodic maintenance of security systems and applications to ensure new threats are identified and managed and the security of the

organisation's assets are maintained;
- Implements and maintains processes for safeguarding physical security of computer & network facilities;
- Conducts research on network and security products, services, protocols, and standards to remain abreast of developments in the networking industry;
- Identifies and plans for Network and Security process improvement initiatives in keeping with the mandate of the organisation;
- Develops mechanisms to manage reform and change, by implementing change management processes, that clarify purpose and the benefits of continuous improvements;
- Maintains linkages with international organisations to keep abreast of trends in ICT that impact directly on the portfolio responsibilities of the agency;
- Keeps current with the latest technologies and determine what new technology solutions and implementations will meet business and system requirements.

Human Resource Responsibilities

- Provides management through effective planning, delegation, communication, training, mentoring and coaching of high-performing audit professionals who possess outstanding knowledge, experience, ethics, and integrity;
- Evaluates and monitors the performance of staff in the Branch and implements appropriate strategies;
- Coordinates the development of individual work plans and recommends performance targets for the staff assigned;
- Participates in the recruitment and training of staff of the Division;
- Recommends succession initiatives, transfer, promotion and leave in accordance with established Human Resource Policies and Procedures;
- Identifies skills/competencies gaps and contributes to the development and succession planning for the Division to ensure adequate staff capacity;
- Monitors the performance of staff and facilitates the timely and accurate completion of the staff annual performance appraisals and other periodic reviews;
- Ensures the well - being of staff supervised;
- Effects disciplinary measures in keeping with established guidelines/practices;
- Demonstrates and upholds the Agency's core values in personal and professional behaviours to minimise 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 new ICT Security Solutions to enhance the agency's

strategic and technical capabilities;
- Engages a range of related stakeholders;
- Recommends staff appointments, promotion, recruitment, disciplinary action, leave and general welfare issues;
- Recommends relevant training and development programmes for direct reports to enhance knowledge and performance.

Performance Standards:

- ICT Security risks mitigated in accordance with established guidelines, agreements and timeframes;
- Cyber security strategies managed in accordance with established guidelines, agreements and timeframes;
- ICT Infrastructure and Applications Audited in accordance with agreed standards, industry guidelines and timeframes;
- ICT Security breaches reported and investigated in keeping with established standards, SLAs and timeframes;
- Recommendations and or advice on ICT security matters provided are evidence-based (supported by qualitative/quantitative data) and delivered within agreed timeframes.
- 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;
- Staff coached and appraisals completed and submitted in accordance to agreed timeframes and standards;
- 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, Corporate Management Director, ICT	• 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 issues and priorities.
Senior Executives/Management in Divisions	• Develop and maintain effective working relationships • Collaborate, exchange information, provide strategic ICT Security Management advice, support and feedback
Direct Reports	• Provide coaching, guidance and support.
General Staff	• 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	• 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	• Develop and maintain effective relationships; • Receive expert advice; and provide and exchange information; • Liaise on key ICT Security Management issues.
Professional Affiliations	• Provides expert advice and exchange information; • Identify innovation and new opportunities for the Association.
Contractors, suppliers and providers of services	• Monitors TOR for goods and services and related interventions; • Exchange of information.
General Public	• 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:

- Sound knowledge of LAN, WAN, and WLAN design and implementation;
- Good Knowledge of network capacity planning, network security principles, and general network management best practices;
- Good knowledge of core routing and switching design principles, best practices, and related technologies;
- Working technical knowledge of current network hardware, protocols, and Internet standards, including routers, switches, firewalls, remote access,

DNS, VLAN, DSL, and Ethernet;
- Excellent 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;
- Sound knowledge of standards and procedures in the development and implementation of ICT systems;
- Sound knowledge of the local and international ICT systems environment, including standards, practices and trends;
- Ability to manage a range of projects types and complex business initiatives and change programmes;
- Good Knowledge of GOJ ICT systems (existing and emerging)
- Strong ability to synthesize multiple ideas and complex information into a coherent summary, as in reports and briefing notes, and to make cogent recommendation for the modification or creation of legislation, policies and programmes;
- 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;
- Five (5) years related experience, with at least three (3) years in an ICT Security/Protection role.

OR

- Certified Information Security Manager (CISM) certification or related ICT security certification;
- Five (5) years related experience, with at least three (3) years 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;
- Five (5) years related experience, with at least three (3) years in an ICT Security/Protection role.