CIVIL SERVICE OF JAMAICA
JOB DESCRIPTION AND SPECIFICATION
COURT ADMINISTRATION DIVISION

JOB TITLE:	ICT Security Officer
JOB GRADE:	MIS/IT 5 /Band 8
DEPARTMENT/DIVISION:	Court Administration Division
BRANCH	Information & Communications Technology Branch
REPORTS TO:	Director – ICT Security
ACCOUNTABLE TO:	Director – ICT Security
MANAGES:	N/A

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

1. STRATEGIC OBJECTIVES OF THE DIVISION

To design, operate, and continuously improve secure, reliable, and innovative information and communications technology systems that enable the efficient delivery of court services, support timely and sound judicial decision-making, strengthen access to justice, and enhance stakeholder confidence in the Judiciary.

2. JOB PURPOSE

Under the leadership and management of the Director – ICT Security, the ICT Security Officer is responsible for developing, implementing and monitoring of ICT Security strategy, frameworks, policies and guidelines, ensuring that the Judiciary successfully manages its compliance and obligations under the GOJ ICT Policies, Standards and Guidelines 2018.

The Information Systems Security Specialist will also maintain the security of all the networks and systems of the Jamaica Judiciary and participate in the effective planning, development and implementation of policies related to the protection of the Judiciary of Jamaica Information Technology (IT) infrastructure. The Information Systems Security Specialist is also expected to provide technical response and investigation capabilities in support of the Jamaica Judiciary.

3. KEY OUTPUTS

- ICT Security processes documented and maintained
- ICT Security infractions and violations monitored and analyzed
- ICT Breaches investigated and reported
- Annual/Quarterly/Monthly/Periodic Reports prepared
- Technical advice and interpretation provided
- Knowledge sharing sessions
- Threat detection strategies
- Individual Work Plan developed

4. KEY RESPONSIBILITY AREAS

Technical/Professional Responsibilities

- Provides technical expertise to support the effective functioning of the Jamaica Judiciary.
- Assists with the identification of the sources of external incidents and propose controls to minimize risk;
- Responds to and investigates computer security incidents using appropriate analysis tools;
- Researches and collects information and documentation required for and or related to all Cyber Security activities;
- Produces security advisories that cater for specific targeted audiences;
- Develops security alerts and bulletins;

- Assists with conducting risk assessment and security analysis on the reported incidents;
- Assists in developing training modules and technical documentation;
- Conducts knowledge sharing sessions among other technical personnel on lessons learnt or new findings;
- Analyses logs and other digital content of systems;
- Maintains up-to-date baselines for the secure configuration and operations of all in-place devices;
- Monitors all in-place security solutions for efficient and optimal operations;
- Reviews logs and reports of all devices and endpoints, whether they are under direct control (security tools) or not (workstations, servers, network devices, etc.); interprets the implications of that activity and formulates plans for appropriate and timely resolution;
- Assists in the design and execution of vulnerability assessments, penetration tests and security audits.
- 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).
- 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.
- Develops and implements security policies, standards, and guidelines to protect the Judiciary's information assets.
- Conducts regular risk assessments to identify vulnerabilities and recommend mitigation strategies to address potential threats.
- Manages incident response protocols to effectively respond to security breaches and incidents.
- Provides assistance to other ICT teams in troubleshooting problems relating to products/solutions.
- 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.
- Monitors security systems and perform regular audits, system backups and recovery to ensure compliance with security policies and standards.
- Develops and tests disaster recovery and business continuity plan to ensure the organization can recover from security incidents.
- 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.
- Organizes and conducts training programmes for employees to raise awareness about cybersecurity threats and best practices.
- Assists with security breach investigations to guide the refinement of information security policies and practices.
- 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 Judiciary.
- 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 Judiciary.
- Ensures that the Judiciary complies with relevant laws, regulations, and industry standards related to ICT security.
- Provides regular verbal and written reports to senior executives on ICT service levels, planned maintenance, issues and data.
- Keeps current with the latest technologies and determine what new technology solutions and implementations will meet business and system requirements.

Management/Administrative 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.
- Plans, executes, assesses and monitors all tasks assigned;
- Produces periodic or ad-hoc reports of high quality for every incident, security threat and vulnerability;
- Implements Cyber Security strategies and policies;
- Provides technical advice in support of the Judiciary of Jamaica Cyber Security policy, strategy, guidelines, standards and best practices;
- Assists with the development of standard operating procedures for handling future types of cyber incidents.
- Assists with the development of guidelines for the Judiciary of Jamaica.
- Keeps abreast of evolving cyber threats and utilising his/her skill and knowledge to identify new and more sophisticated approaches to detecting threats;
- Assists with ensuring compliance with the Judiciary of Jamaica guidelines, standards and requirements;

Human Resources 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.

Other Responsibilities

- Performs all other duties and functions as may be required from time to time.

5. PERFORMANCE STANDARDS

- ICT Security processes documented and maintained in keeping with industry standards, GOJ guidelines and timeframes.
- ICT Security infractions and violations monitored and analyzed in keeping with industry standards, GOJ guidelines and timeframes.
- ICT Breaches investigated and reported in keeping with industry standards, GOJ guidelines 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 the agreed format, are accurate and submitted on time.
- Individual Work Plans developed in conformity with established standards and within agreed timeframes.
- Staff coached and appraisals completed and submitted in accordance with agreed timeframes and standards.
- Confidentiality, integrity and professionalism displayed in the delivery of duties and interaction with staff.

6. AUTHORITY

- Recommends ICT Network and Security strategies and programmes.
- Investigates ICT Security breaches.

7. INTERNAL AND EXTERNAL CONTACTS (specify purpose of significant contacts)

Internal Contacts

Contact (Title)	Purpose of Communication
Senior Director – ICT Director – ICT Security	• Provide advice and contribute to decision making. • Identify emerging issues/risks and their implications, and propose solutions. • Receive guidance and provide regular updates on

Contact (Title)	Purpose of Communication
	key ICT Security issues and priorities.
Senior Executives/Management	• Develop and maintain effective working relationships • Collaborate, exchange information, provide strategic advice, support and feedback
Public Procurement	• Develop and maintain effective working relationships on matters public procurement management and financial resourcing
General Staff	• Develop and maintain effective relationships • Provide expert advice and exchange information

External Contacts

Contact (Title)	Purpose of Communication
MDAs Key Stakeholders – Police, TAJ, DCS, DPP, EOJ, etc.	• Develop and maintain effective relationships. • Receive expert advice; and provide and exchange information. • Liaise on key Court Operations and Management Support & ICT Security issues.
Office of the Cabinet	• Develop and maintain effective relationships. • Receive expert advice; and provide and exchange information. • Liaise on key ICT Security issues.
Auditor General	• Exchange information on audit queries and related processes
Committees of Parliament related to Corporate Services/HRMD Affairs	• Assists/Supports the CEO in discussions on the Judiciary's ICT Security and related matters
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.

8. REQUIRED COMPETENCIES

Core

- Excellent interpersonal and team management skills
- Excellent communication skills
- Strong analytical and problem-solving skills

- Strong leadership skills
- Strong customer relations skills
- Excellent planning and organizing skills
- Excellent judgment and decision-making skills
- Ability to influence and motivate others
- Proficiency in the use of relevant computer applications

Technical

- 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 systems 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 project 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 recommendations for the modification or creation of legislation, policies and programmes.
- Good verbal and written communication skills, with the ability to deliver presentations with tact, clarity, enthusiasm and accuracy to widely varied audiences.
- A high level of initiative and self-motivation.
- Demonstrated interpersonal and negotiation skills

9. MINIMUM REQUIRED EDUCATION AND EXPERIENCE

- Bachelor's degree in **Information Technology, Computer Science, Cyber Security, Information and Communications Technology, Computer Engineering**, or a related discipline from a recognised tertiary institution.
- **A minimum of three (3) years' experience** in ICT **security or Network Administration/security role**.
- **Training and/or professional certification** in Information Security or Cyber Security (e.g. CEH, CHFI, CISSP, GCIA/GCFA, or equivalent) would be an asset.
- Practical exposure to **ICT security operations, monitoring, or incident response** will be an asset.

OR

- **NVQJ Level 5** in Computing, Software Design, Computer Science, ICT, Management Information Systems, Computer Engineering, or a related discipline.
- **A minimum of three (3) years' experience** in ICT **security or Network Administration/security role**.
- Training and/or professional certification in **Cyber Security or Information Security** (e.g. CEH, CHFI, CISSP, GCIA/GCFA, or equivalent) would be an asset.

10. SPECIAL CONDITIONS ASSOCIATED WITH THE JOB

- 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.
- MUST own or have access to a reliable motor vehicle.
- Will be required to travel locally to perform ICT infrastructure and security functions at outstations and to attend conferences, seminars and meetings.