CIVIL SERVICE OF JAMAICA

MINISTRY OF SCIENCE, ENERGY AND TECHNOLOGY

Job Description and Specification

JOB TITLE:	Cyber Analyst/Researcher
JOB GRADE:	MIS/IT 7
POST #:	71166
DIVISION:	Cyber Incident Response Team (CIRT)
REPORTS TO:	Director, CIRT
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

JOB PURPOSE

Under the direction of the Director, CIRT the Cyber Analyst/Researcher will conduct cyber research and develop technical mechanisms for internal use and training, as well as perform monitoring tasks geared towards the development of tools to manage cyber threats.

The incumbent will also participate in the effective planning, development and implementation of policies related to the protection of the Government of Jamaica's (GoJ) Information Technology (IT) infrastructure as well as other national critical IT Infrastructures. The Cyber Analyst/Researcher is also expected to provide technical response and investigation capabilities in support of the CIRT.

KEY OUTPUTS

- Laboratory management
- Risks assessment
- Operational policies and procedures
- Training modules and technical documentations
- Knowledge sharing sessions
- Technical advice
- Technical reports
- Projects/programmes monitoring mechanisms
- Research and development
- Security analysis
- Threat detection strategies
- Research tools and systems
- Analysis (Statistical, malware, forensic)

KEY RESPONSIBILITY AREAS

Management/Administrative

- 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 strategy and policies.
- Provides technical advice in support of the GoJ cyber security policy, strategy, guidelines, standards and best practices.
- Assists with the development of standard operating procedures for handling future types of cyber incidents by GoJ Ministries, Departments and Agencies (MDAs) such as guidelines and protocols for the conduct of GoJ's staff.

- Assists with the development of guidelines for the regulation of national IT security industry, contributes to the development of Information Security related policy, strategy, guidelines, standards and best practices within the public sector.
- Performs proactive engagement in order to identify potential threats to the environment and its customers.
- Keeps abreast of evolving cyber threats and utilising his/her skills and knowledge to identify new and more sophisticated approaches to detecting threats.
- Assists with ensuring compliance with GoJ cyber security guidelines, standards and requirements.
- Contributes to the preparation of the Budget and Operational Plan for the CIRT.

Technical/Professional

- Provides technical expertise to support the effective functioning of the CIRT.
- Assists with the identification of the sources of external incidents and propose controls to minimize risk.
- Investigates computer security incidents using appropriate analysis tools.
- Researches and collects information and documentation required for and or related to all cyber security activities.
- Conducts risk assessment and security analysis on the reported incidents.
- Responds and provides support to the MDAs.
- Assists in developing training modules and technical documentation.
- Conducts knowledge sharing sessions among other technical personnel on lessons learnt or new findings.
- Monitors all in-place security solutions for the CIRT 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.
- Provides on-call support for end users for all in-place security solutions.
- Perform proactive assessment (e.g. threat hunting), as well as, confidential investigation and digital forensics capability.

Human Resource

- Attends Department/Ministry staff meetings, as required.

Other

- Performs any other duties assigned from time to time.

INTERNAL AND EXTERNAL CONTACTS

Internal	***Nature of Relationship***
Director, CIRT	Instructions, guidance, work assignment, advice and sharing information
All staff members	Advice, sharing information and addressing concerns
External	***Nature of Relationship***
ICT staff in other Ministries/Agencies Departments and the	Professional advice, guidance, reports, information sharing
Private Sector	Advice and sharing information

PERFORMANCE STANDARDS

- Deliverables are produced within an agreed timeframe and to required standards.
- A team approach is adopted in an effort to improve the effectiveness and efficiency of the CIRT's objectives.
- Is aware of and complies with all policies, procedures and guidelines.
- Integrity, confidentiality and professionalism are maintained in the execution of duties.

REQUIRED COMPETENCIES

The Performance Management and Appraisal System: Guideline System and Reference Manual – Competency Framework informed the following with grade '1' being the lowest and '3' or '4' the highest.

Core	**Level**	**Functional**	**Level**
Oral communication	4	Initiative	3
Written communication	4	Use of technology (relevant computer applications such as Microsoft Office suite	2
Customer and quality focus	4	Managing external relationships	3
Team work and cooperation	3	Strategic vision	3
Interpersonal skills	3	Problem solving and decision making	3
Compliance	3	Analytical thinking	4
Integrity	4	Goal/result oriented	3
Change management	2	Planning and organizing	3
Adaptability	3	Methodical	3
		Impact and influence	2

		• Sound knowledge of computer hardware. • Knowledge of systems development • Knowledge of at least 2 operating systems (UNIX and Windows). • Excellent knowledge of at least 3 programming languages (Python, BashShell, PHP, C++, Java, etc.) • Knowledge of internet applications. • Knowledge of security risks, threats and vulnerabilities. • Excellent knowledge of risk assessments. • Excellent knowledge of cryptographic technologies. • Ability to exercise sound judgment and conviction of purpose in unfavourable or unpopular situations. • Sound knowledge of the general operations of the machinery of government. • Ability to manage limited resources in order to achieve challenging output targets. • Good records management skills. • Project management skills.

MINIMUM REQUIRED QUALIFICATION AND EXPERIENCE

- Bachelor's Degree in Computer Science/ Information Technology/ Information Communication Technology/Telecommunications/Engineering–Electronics or any relevant area from a recognized tertiary institution; plus
- At least five (5) years working experience in Information Technology, Project Development and Cyber Security.
- Professional certification/training in any related field such as Computer Forensics, CISM, CISA, CISSP/GCIA /GCFA/CEH/CHFI or any related field and experience in Research and Development would be an asset.

SPECIAL CONDITIONS ASSOCIATED WITH THE JOB

- Regularly required to travel within the country regarding cyber security matters.
- Maybe be required to work beyond regular working hours.

AUTHORITY

N/A