Office of the Services Commissions
(Central Government)
Ministry of Finance and the Public Service Building
30 National Heroes Circle, Kingston 4
Jamaica, West Indies
Tel: 876-922-8600
Fax: 876-924-9764
Email: communications@osc.gov.jm
Website: www.osc.gov.jm

CIRCULAR No. 397 **19th September, 2022**
OSC Ref. C. 6528[12]

Permanent Secretaries, Heads of Department and Chief Executive Officers are asked to invite applications from suitably qualified officers in their Ministries/Departments/Agencies to fill the following **vacant** posts in the **Cyber Incident Response Team Division, Ministry of Science, Energy and Technology**:

1. **Information Systems Security Specialist (MIS/IT 7)**, salary range $2,622,489 - $3,117,316 per annum and any allowance(s) attached to the post.

2. **Cyber Analyst/Researcher (MIS/IT 7),** salary range $2,622,489 - $3,117,316 per annum and any allowance(s) attached to the post.

1. Information Systems Security Specialist (MIS/IT 7)

Job Purpose

Under the direction of the Head, Cyber Incident Response Team (CIRT), the Information Systems Security Specialist will manage and maintain the CIRT Networks and Systems, IDS and ISP and will manage access to information and assist with responding to incidents when networking and systems expertise are needed.

The incumbent will also maintain the security of all the networks and systems of the CIRT and participate in the effective planning, development and implementation of policy related to the protection of the Government of Jamaica's (GoJ) Information Technology (IT) infrastructure as well as other national Critical IT Infrastructures. The Information Systems Security Specialist is also expected to provide technical response and investigation capabilities in support of the CIRT.

Key Responsibilities

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, contribute to the development of Information Security related policy, strategy, guidelines, standards and best practices within the Public Sector;
- 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 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;
- 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;
- 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;
- Analyzes logs and other digital content of systems;
- Manages and updates the CIRT's Web Portal;
- Manages file servers;
- Maintains up-to-date baselines for the secure configuration and operations of all in-place devices;
- Monitors all in-place security solutions for the CIRT for efficient and optimal operations;
- Reviews logs and reports on 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.

Human Resource Management:

- Attends Department/Ministry staff meetings, as required;
- Performs any other related duties that maybe assigned from time to time.

Required Knowledge, Skills and Competencies

Core:

- Good oral and written communication skills
- Customer and quality focus
- Teamwork and co-operation
- Good interpersonal skills
- Compliance
- Integrity
- Change management
- Adaptability

Functional:

- Ability to work on own initiative
- Use of technology (relevant computer applications such as Microsoft Office suite
- Managing external relationships
- Strategic vision
- Good problem-solving and decision-making
- Analytical thinking
- Goal/result oriented
- Good planning and organizing skills
- Methodical
- Impact and influence
- Possess high degree of interest in ICT security related areas
- Sound knowledge of computer hardware
- Knowledge of at least 2 operating systems (UNIX and Windows)
- 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 Information Technology/Computer Science/Information Communication Technology/Engineering – Electronics, Telecommunications/any relevant area from a recognized tertiary institution;
- Five (5) years working experience in a relevant IT field and in Systems Administration;
- Professional certification/training in any related field such as Cyber Security and Cyber Security Incident Response, CISSP/GCIA /GCFA/CEH/CHFI is an added advantage;
- One (1) year experience working in the field of Cyber Security 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.

2. Cyber Analyst/Researcher (MIS/IT 7)

Job Purpose

Under the direction of the Head, Cyber Incident Response Team, 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 Responsibilities

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 proposes 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;
- Performs proactive assessment (e.g. threat hunting), as well as, confidential investigation and digital forensics capability.

Human Resource:

- Attends Department/Ministry Staff Meetings, as required;
- Performs any other related duties that may be assigned from time to time.

Required Knowledge, Skills and Competencies

Core:

- Good oral and written communication skills
- Customer and quality focus
- Teamwork and co-operation
- Good interpersonal skills
- Compliance
- Integrity
- Change management
- Adaptability

Functional:

- Ability to work on own initiative
- Use of technology (relevant computer applications such as Microsoft Office suite
- Managing external relationships
- Strategic vision
- Good problem-solving and decision-making
- Analytical thinking
- Goal/result oriented
- Good planning and organizing skills
- Methodical
- Impact and influence
- Sound knowledge of computer hardware
- Knowledge of systems development
- Knowledge of at least two (2) operating systems (UNIX and Windows)
- Excellent knowledge of at least three (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;
- 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.

Applications accompanied by résumés should be submitted **no later than Friday, 30th September, 2022 to:**

Director, Human Resource Management and Development
Ministry of Science, Energy and Technology
PCJ Building
36 Trafalgar Road,
Kingston 10

Email: careers@mset.gov.jm

Please note that only shortlisted applicants will be contacted.

Please ensure that a copy of this circular is placed at a strategic position on the Notice Board of the Ministry/Department/Agency and brought to the attention of all eligible officers.

Merle I. Tam (Mrs.)
for Chief Personnel Officer