

POSITION DESCRIPTION

Job Title: Manager, Computer Security Incident Response Team (CSIRT)

Ministry: Ministry of National Security

Unit: Computer Security Incident Response Team (CSIRT)

Reports to: Deputy Permanent Secretary, Ministry of National Security

Supervising: ICT Security Specialists
Business Operations Assistant II

Role: The incumbent will be required to perform as the MNS's Project Manager for the project implementation process, and will be also required to manage a team of technical professionals in order to successfully implement the CSIRT. Upon establishment of the CSIRT, the Manager will develop and implement operational policies, processes and procedures relating to incident response and management; and develop and chart the strategic direction for the continued operation of the CSIRT in accordance to international best practices.

Duties and Responsibilities:

Project Implementation Duties 0-9 months

- Manages the implementation of the CSIRT – TT for the Government of Trinidad and Tobago by working directly with the International Telecommunication Union's (ITU) Project Team.
- Serves as the on-site contact to the ITU team personnel and provide the MNS with periodic status reports of project.
- Schedules tasks and assignments of personnel on the MNS project team, drafting reports, and acts as the first line of communication between the MNS project team and the ITU project team as it relates to any project issues.
- Procures and installs all hardware and infrastructure required for the successful implementation of the project.
- Prepares the required project documentation, status updates, reports and configuration information produced as by-products of the project.

Operational Duties - 9 – 36 months

- Manages the daily operations of the CSIRT, including staffing, budgeting and other relevant management functions, and provides specific technical expertise for functions supervised.
- Manages and leads a team of professionals in Incident Response and Management and ensures the discharging of respective functions in accordance with established policies and procedures.
- Develops strategic goals and objectives of the CSIRT.
- Plans and manages the budget required for CSIRT operations.

- Advises the Director of the Trinidad and Tobago Cyber Security Agency on all matters related to Computer Security Incident Response Management.
- Ensures all incidents are processed quickly and accurately and classified, prioritized and escalated appropriately when necessary.
- Provides overall direction during execution of the incident response process, providing advanced analysis and direction.
- Consults with and advises other Unit heads on cyber security needs and issues.
- Develops a framework for the creation and implementation of CSIRTS for GORTT Ministries and Agencies.
- Coordinates the implementation of CSIRTs in all GORTT Ministries and Agencies.
- Liaises with all local CSIRTs to treat with cyber security incidents to coordinate effective incident response.
- Liaises with the National Operations Center and serves as the Point of Contact to facilitate information exchange on pertinent issues related to cyber intelligence.
- Coordinates with other international CSIRTs or related organizations dedicated to the management of cyber incidents
- Directs completion of post mortem analysis, document findings and provides recommendations to proper security and infrastructure teams.
- Defines scope of physical security penetration tests, coordinates and communicates with appropriate teams and management.
- Creates and provides reports to management regarding the performance of incident management and the state of network and data security from an operational level.
- Prepares and submits status reports on the operations of CSIRT –TT.
- Performs other related duties are required.

Knowledge, Skills and Abilities:

- Knowledge of IT end-to-end problem management and root cause analysis.
- Knowledge of and an active interest in: information security research; computer industry trends; telecommunications; virtualization, and mobile computing.
- Proficiency in working in a fast-paced, complex, dynamic, multicultural business environment.
- Excellent leadership skills

- Strong communication skills with a proven ability to understand key concepts and communicate with technical staff, and senior management.
- Strong negotiating skills
- Strong analytical and problem-solving skills.
- Understanding of IT Service Management processes.
- Strong organizational skills and the ability to perform in a command-and-control role under pressure, and the ability to manage multiple priorities with competing demands for resources.
- Ability to consume and synthesize intelligence about actors, techniques or situations to identify emerging risk scenarios.
- Proficiency in process formulation and improvement.

**Qualifications
& Experience:**

- Bachelor's degree in Information Technology, Computer Science, Electrical Engineering or closely related field is required
- Master's degree in Information Technology, Management Information Systems, Management or closely related field is required.
- Professional certification and \ or training in one or more of the following; Computer Security, Computer Security Incident Response and Management, IT Auditing, CISSP,CISM,CISA, ISO 2700 or BS 7799.
- Minimum of five years mid to senior level working experience
- Professional certification in Project Management
- Some experience in the management and administration of IT related projects.
- Three years experience in the management of Information Systems.
- Three to five years working experience with an international or regional organization will be an asset.
- Must be positively vetted.