| GPL-IT-JMD | OUTPUT FOCUS JOB DESCRIPTION | | Information Technology Division |
|---|---|---|---|
| **Position: Cybersecurity Officer** | **Grade: JM-'D'** | **Incumbent:** | **Reports to: Manager – IT Infrastructure** |
| **Manages:** - | | | |

**JOB PURPOSE:** **To develop and maintain an industry standard corporate Cybersecurity framework support the protection of the corporate IT and OT Infrastructure, applications and data from cybersecurity breaches. This framework is also required to effectively inform the continuous planning, implementation and execution of policies, procedures and corporate end user awareness.**

**KEY OUTPUTS:**

- ✓ Cybersecurity Strategy
- ✓ Cybersecurity policies and procedures
- ✓ Cybersecurity Monthly report
- ✓ Cybersecurity Audit and Risk assessment reports (inclusive of NIST core functions)
- ✓ Cybersecurity awareness and guidance memoranda
- ✓ Antivirus and Malware protection statistics

**KEY RESPONSIBILITY AREAS:**

1. Produce monthly and on demand Cybersecurity audit/assessment reports that identify gaps and recommend remedial strategies.
2. Produce Cybersecurity policies, standards, baselines, guidelines and procedures that ensure consistency, predictability and resilience in the management, monitoring and protection of corporate IT and OT infrastructure.
3. Establish and executes (in collaboration with the Human Resources Development Department) comprehensive cybersecurity awareness training programs to enhance the overall awareness level within GPL.
4. Ensure dissemination of Cybersecurity memoranda to ALL Staff to foster a Cybersecurity conscious GPL workforce.
5. Coordinate and support authorized Penetration Testing on GPL's ICT infrastructure and related assets.
6. Develop and maintain methods to monitor and measure cybersecurity risk, compliance, and assurance efforts.
7. Establish and maintain systems to mitigate Cyberattacks within the NIST framework of: Identification, Protection, Detection, Response and Recovery.
8. Interpret patterns of end-user and system non-compliance to determine impact on levels of risk and/or overall effectiveness of the GPL's cybersecurity program.
9. Maintain up-to-date knowledge of cybersecurity issues including awareness of emerging security threats, solutions, services, protocols, and standards in support of GPL's IT infrastructure security enhancement efforts.
10. Maintain and demonstrate knowledge of applicable policies, regulations, and compliance documents specifically related to cybersecurity audits/assessments
11. Perform other related tasks that may be required from time to time to achieve Divisional and corporate objectives.

Required Competencies

| Core/ Leadership | Skill Level & Importance | | Description/Behaviours |
|---|---|---|---|
| Adaptability & Managing Change | H | 3 | • Helps others adapt to a changing work environment and to embrace change.<br>• Promotes the benefits of a proposed change.<br>• Takes time to question, understand and speak to the underlying needs of stakeholders beyond those initially expressed.<br>• Makes/recommends changes to work processes or systems to improve business results.<br>• Develops plans and prioritizes resources to effectively implement change.<br>• Remains focused on the desired outcome to help self and others implement change. |
| Decision Making Analysis and Problem Solving | H | 2 | • Applies guidelines and procedures that require some interpretation when dealing with exceptions.<br>• Makes appropriate independent decisions in non-routine situations.<br>• Considers the risks and consequences of action and decisions.<br>• Focuses on innovative rather than ordinary solutions to problems.<br>• Monitors impact and effectiveness of decisions. |
| Financial Responsibility and Value Creation | H | 2 | • Understands the current costs of work processes and programs.<br>• Balances cost versus benefit in taking action or making cost related decisions.<br>• Prepares accurate cost estimates and schedules.<br>• Monitors the budget, tracks costs and revenue, where appropriate.<br>• Takes corrective action as required.<br>• Monitors to ensure the efficient and appropriate use of resources.<br>• Continuously looks for methods to improve operational efficiencies. |
| Safety Focus | H | 2 | • Proactively thinks about his/her safety and the safety of others.<br>• Keeps personal and group safety on employees' minds at all times.<br>• Adheres to high personal standards of safety<br>• Reports and/or corrects unsafe work conditions.<br>• Acts to correct unsafe work habits.<br>• Documents and monitors occupational safety and health violations. |
| Teamwork Oriented | H | 3 | • Proactively solicits ideas and opinions and shares information and learning with others.<br>• Addresses conflicts or issues within the team in a positive and open manner.<br>• Provides clear feedback to team members.<br>• Uses understanding of different interests and agendas to achieve positive outcomes.<br>• Engages others in collaborative problem solving, encouraging them to share their ideas and opinions.<br>• Is open, sincere, and empathetic in dealing with all individuals and in all circumstances. |
| Leading and Managing People | H | 2 | • Give others opportunities to practice new skills and provides or arranges coaching.<br>• Works to provide a supportive environment by securing necessary resources and removing blocks to effective working.<br>• Expresses confidence in the ability of others to be successful.<br>• Recognizes employee development needs and opportunities, provides on-going feedback and coaching. |

**Technical/ Functional Competencies**

| Technical/Functional | Skill Level B, W, A,E | 1,2,3,4 |
|---|---|---|
| ➢ Strong Cybersecurity and organizational skills. | **A** | **3** |
| ➢ Must be self-motivation, adaptability and a positive attitude | **W** | **3** |
| ➢ Ability to analyse and resolve problems. | **A** | **3** |
| ➢ Knowledge of ISO Policy and Procedures | **W** | **3** |
| ➢ A good working knowledge of established Cybersecurity practices and deployment of key practices | **W** | **3** |
| ➢ Be familiar with NIST, ISO 27001 and NERC CIP | **W** | **3** |
| ➢ Ability to handle multiple tasks simultaneously and keep accurate records. | **A** | **3** |

**MINIMUM REQUIRED EDUCATION AND EXPERIENCE**

Bachelor's Degree in Cybersecurity, Information Assurance, Information Systems, Computer Engineering, Computer Science, or a related discipline from a recognised university.

**PLUS**

A minimum of three (3) years of relevant experience in securing data and communications networks and the development of Security Resilient Information Systems architecture and solutions.

In addition, the candidate must possess one (1) or more of the following or similar certifications: CompTIA Security+, ISACA Certified Information Systems Auditor (CISA), $(ISC)^2$ Certified Information Systems Security Professional (CISSP), $(ISC)^2$ System Security Certified Practitioner (SSCP), ISACA Certified Information Security Manager (CISM), EC-Council Certified Security Analyst (ECSA) or related certification.

***Legend:***

| | |
|---|---|
| **H:** | High Requirement. Required performance could not be achieved without demonstration of this competency. |
| **M:** | Medium Requirement. Required performance would be difficult to attain without demonstration of this competency. |
| **L:** | Low Requirement. Required performance is not dependent on demonstration of this competency. |
| **I,II,III,IV:** | The skill level required for effective performance. Skill levels are defined in the Competency Model |
| ***** | If a formal leader, all leadership competencies will apply. A formal leader is primarily responsible for the leadership and/or supervision of others. Duties are generally different than the duties of the others in the group. |
| **B:** | Basic – Brief, general familiarity. Understanding of where knowledge can be applied, but limited on-the-job application. |
| **W:** | Working – Detailed familiarity and understanding. Proficient in applying the knowledge and skills for regular job requirements. |
| **A:** | Advanced – Comprehensive understanding (in-depth familiarity with fine points). Able to handle complex or non-routine applications. |
| **E:** | Expert – Comprehensive and conceptual understanding. Expert, "go to" resource, can handle highly complex problems or Situations. |

**This document is validated as an accurate and true description of the job as signified above.**

| | |
|---|---|
| Employee Sign | Date |
| Supervisor Sign | Date |
| Head of Department/Division | Sign Date |
| Date received in Human Resource Division | Date Created/revised |