**Job Description**

**Job Title: IT Security Engineer**

**Career Level: 5**

**Department or Business Sector: Information Systems**

**Location**: **Ansty Park**

**Reporting to (manager’s job title): Infrastructure and Operations Manager**

***Please read the notes on pages 2 and 3 before completing these sections.***

|  |  |
| --- | --- |
| **Heading:** | **Description** |
| 1. **Job Purpose**
 | We are looking to recruit an IT Security Engineer to assist in the delivery of the IT departments security strategy along with being responsible for performing routine security analysis of the environment, reporting on current security posture, and investigation alerts generated from our systems. The role will also require conducting of research to keep up with current security trends and advise on mitigation options. Working collaboratively with other departments in the business in order to understand security requirements of both departmental and colleague's individual needs. Confidentiality and discretion will be required as the role will also assist with subject access requests. |
| 1. **Communication**
 | The IT Security Engineer will be able to * Communicate in technical terms with colleagues within the IT function.
* Where necessary liaising with 3rd parties
* Create clear, engaging end user communications that allow staff to understand our security principles
 |
| 1. **Innovation**
 | The IT Security Engineer will * Setup, deploy, and maintain various security technologies to defined specifications / configurations
* Provide recommendations and assist in the remediation and hardening of various systems, and validate the implementation
* Document processes and procedures to ensure compliance and quality of system operating procedures
* Define configuration policies and tuning of the information and event monitoring tools
* Advise and influence security principles adopted by the business and as part of project delivery
* Monitor device and service compliance status and policy deployment
* Assist in the building and deployment of various phishing simulations and training campaigns and other security activities to improve protection from social engineering
 |
| 1. **Knowledge**
 | The IT Security Engineer will have good knowledge of * Security within Operational Technology environments.
* CE Plus auditing process and requirements
* Windows/Linux servers’ deployment and maintenance
* A good understanding of Microsoft cloud-based security products and their configuration
* Experience of VPN and CASB solutions
* Understanding of IAM/PAM principles
* Experience with managing both on premises and cloud-based applications.
* Experience of working with and securing Azure/AWS environments
* Implementation and management of security best practices
* Experience working within an ITIL environment
 |
| 1. **Person Specification**
 | All aspects of the role are to be carried out as an exemplar within the business in adhering to the MTC RIGHT way:* Acting responsibly, putting MTC’s interests ahead of personal ambition.
* Delivering in the broadest sense a great working environment.
* Promoting teamwork, supporting through challenging times and collectively celebrating our successes.

In addition:* Past work experience of working within a dedicated security focused role
* Enthusiasm and self-motivation for continuous learning and pursuing further
* A problem-solving approach to identify how the MTC can operate and innovate securely
 |

**Definitions**

**1. Job purpose:**

*Provide an overview of the job, its context in the company.*

*Describe the level and scope of influence and authority that the position should have (is this within the immediate job area or more widely across a business unit or potentially the business as a whole?).*

*Describe the level of impact by reference to the daily scope of the role – does the role holder follow clearly defined procedures under close supervision or is there latitude to set objectives or even strategies?*

**2. Communication:**

*Outline the scope, extent, and nature of the communication that this role is responsible for, on a regular basis.*

*What communication skills are required? (To convey information, to reach agreement, to manage communication?);*

*What is the context: internal or external?*

**3. Innovation:**

*To what extent is the role holder required to identify, develop, and make improvements to ideas, techniques, procedures, services or products?*

*What is the level of complexity? (Are problems generally in one area and well defined or are they multi-dimensional?)*

*Is the role holder expected to make minor changes or to enhance or replace entire processes?*

**4. Knowledge:**

*What is the nature and extent, or depth of knowledge required in this job to achieve objectives and add value?*

*Knowledge may be acquired through formal education and/or work experience.*

*First specify the depth of knowledge to be applied and then identify whether the role holder would apply the knowledge as a team member, team leader or manager of teams.*

**5.** **Person Specification:**

*The type of person suitable for the role:*

*For example, does this require someone who enjoys working with lots of detailed data, or someone who enjoys working with customers or potential customers.*

*Would this role be suited to someone with high levels of resilience and an aptitude for working under pressure, to meet deadlines?*

*What sort of prior experience would be necessary or helpful?*