|  |  |
| --- | --- |
|  | |
| **Role title** | Cyber Security Analyst |
|  | |
| **Department** | Cyber Security |
|  | |
| **Business unit or function** | Cyber Security |
|  | |
| **Role reports to** | Cyber Security Manager |
|  | |
| **Roles managed** | N/A |
|  | |
| **Purpose of the role** | |
| The role involves supporting the team by analysing cyber security systems, investigating alerts and escalating possible cyber incidents and breaches. This is a key role for identifying and reporting events to be further investigated.  The ISA will provide valuable cyber security support to the business through identifying, documenting and publishing suitable security tips and tricks. The ISA will also be able to answer questions and provide general guidance from colleagues about methods of staying secure. | |
| **Accountabilities of the role** | |
| * To monitor security systems, reviewing logs and alerts. * Collating metrics and analysing trends. * Reviewing daily reports such as but not limited to : Phishing alerts, End-points compliance queries and Active Directory accounts. * Complete scheduled cyber security audits. * Completing customer cyber security questionnaires. * Assisting with investigating suspected and actual security incidents and breaches, documenting the actions. * Reviewing and republishing cyber policies. * Update cyber security dashboard. * Stay updated with the latest technology trends and security standards. * Research, write and publish cyber tips for colleagues. * Maintain the Information Security Management System (ISMS). | |

**Competencies, Skills, Qualifications & Experience**

**Essential** attributes are the minimum requirement for a role holder. Without these attributes, the role could not be performed. **Desirable** attributes would enable the candidate to perform more effectively, but they are not critical to the role.

|  |  |  |
| --- | --- | --- |
| **Competency, Technical Skill or Knowledge** | **Essential** | **Desirable** |
| Understanding of the business process, application architecture and infrastructure architecture. |  | **√** |
| Strong methodical approach to work. | **√** |  |
| Good risk and situation judgement, leading to balanced escalation. | **√** |  |
| Adheres to procedures at all times. | **√** |  |
| A broad thinker and problem solver. | **√** |  |
| Develop and maintain good partnerships with all business functional departments and 3rd parties. |  | **√** |
| Strong attention to detail. | **√** |  |
| Self-motivated to learn new skills in a changing environment. | **√** |  |
| Understanding of risk concepts and operations. |  | **√** |
| **Qualifications** | **Essential** | **Desirable** |
| Experience with databases, applications and programming software |  | **√** |
| Experience of network structures and concepts. |  | **√** |
| Experience of planning & control of projects. |  | **√** |
| IT Security qualification. |  | **√** |
| **Previous Experience** | **Essential** | **Desirable** |
| At least one year in a Cyber Security / IT Technical role |  | **√** |
| Experience and capability to complete projects, on time on budget delivery. |  | **√** |

|  |
| --- |
| **Organisation Chart** |
|  |