**JOB DESCRIPTION**

|  |  |
| --- | --- |
| **Job title** | Security Analyst |
| **Sector/Function** | IMT – Information Management and Technology |
| **Department** | Security |
| **Reports to** | Head Of Security |
| **Grade** | Grade 4 |
|  |  |
| **Job purpose** | To ensure the relevant levels of security are in place across the Turning Point help to maintain the Information Security Management System (ISMS), provide technical advice to projects, manage the security toolset and provide incident response when needed. Provide a customer-focused service to IMT and the wider business. |
| **Key accountabilities** | **Information Security Management*** Support in writing technical policies and standards as part of the ISMS and promote compliance in line with international security standards (i.e. ISO27001), Public Sector security (i.e. HMG Cyber Essentials, Cloud Security Principles, NHS toolkit and InfoSec Standards), and corporate policies.
* Support in maintaining the ISMS with applicable legislation e.g. Data Protection Act, Computer Misuse act, etc.
* Contribute to the creation and maintenance of relevant security documentation for appropriate systems and on occasion lead IM&T input to these.
* Support the Head of Security to risk assess security in terms of impact to systems and service confidentiality, integrity and availability, and report and escalate results of risk assessments.

**Security Engineering*** Provide security consultancy, advice and guidance to IM&T teams involved in the design, development, delivery and change of TP products and services.
* Assist in the provision of designs and technical solutions in support of corporate security policies and external standards.
* Produce, review and constantly test and evaluate effectiveness and efficiency of technical security controls, configurations standards and procedures in line with security requirements, business needs, delivering enhancements where applicable.
* To be a security representative for all ICT technical deliveries, initiatives and project implementations in the absence of Head of Security

**Security Operations*** Assist in the specification and design of automated security tools and, in conjunction with the IM&T teams, support the installation, configuration of such tools including maintenance and monitoring activities.
* Actively monitor security tools deployed within the TP (anti-virus, configuration control, vulnerability management, IDS/IPS, end point security), escalate issues, assist with remediation and maintain these systems. Ensure that the ICT infrastructure is appropriately patched.
* Provide on call support with particular reference to a security incidents. Keeping IMT aware of the incident and next steps to resolution.
* Ensure the escalation of any real or potential security breaches and vulnerabilities.
* Provide information and leadership to ICT teams during incident response in order that appropriate remedial steps can be taken. Undertake technical investigations as a result of security incident to understand route cause and identify actions to reduce / remove risk.

**General*** This role will involve travel to various locations to support the needs of the business.
* Establish good l relationships with stakeholders to ensure that any security issues are communicated and we are able to assess the level of risk and deploy appropriate solutions.
* Promoting continuous process improvement, in relation to security matters, within IM&T.
 |
|  |
| **Dimensions** | Direct reports | N/a |
| Total staff overseen | N/a |
| Internal contacts | All Business Functions |
| External contacts | Vendors |
| Planning outlook | 12,24 months |
| Problems solved | Technical, governance, data management and integrity |
| Financial authority | N/ a |

**PERSON SPECIFICATION**

|  |  |
| --- | --- |
| **Job title** | Security Analyst |
|  |
| **Personal effectiveness** | Essential | Desirable |
| * An understanding of information security management system(s), e.g. ISO 27001,
* Demonstrable experience in a similar full time security role
* A technical aptitude to understand security of IT systems, networks and security architectures
* Demonstrable knowledge of Risk Management
* Understanding of Asset Management
* Internal Auditing experience in Information Security
* Incident Management and security investigations
* Experience of monitoring the operation of networks, servers and desktops security controls
* Ticket and Request Management
* Evidence of ability to make sound decisions
* Evidence of ability to manage a varied and challenging workload
* Able to effectively communicate verbally and in writing
* Excellent report writing skills
* Ability to effectively prioritize and execute tasks in a high pressure environment
 | * Exposure to Project Management Techniques
* Experience with CISCO, Trend, Alienvault, Forcepoint and other security technologies used by TP
 |
|  |  |  |
| **Technical effectiveness** | Essential | Desirable |
| * Knowledge of Cloud Information Secuirty: SaaS, PaaS, IaaS and inparticular O365, Azure, Oracle
* Understanding hardening techniques and processes e.g. CIS benchmarks
* Knowledge of Cisco ASA capability and configuration, router and switch capability and configuration, and VPN capability and configuration.
* Extensive practical knowledge of Windows server and desktop operating systems, and all aspects of their security and audit controls, particularly Windows 7/10 and Windows Server 2008/2012/2016 and all aspects of its security and audit controls.
* Extensive and demonstrable knowledge of server virtualisation such as VMWare and Hyper V.
* A good understanding of intrusion detection technologies
* Significant practical knowledge of MS-Exchange and all aspects of its security and audit controls.
 |  |
|  |  |  |
| **Acquired experience & qualifications** | Essential | Desirable |
| * Degree qualifications in an IT related discipline, or CISSP, CISA or other relevant security industry certification
 | * ITIL v3 Foundation
* MCSE
 |
|  |  |  |
| **Other requirements** | Essential | Desirable |
|  |  |