|  |
| --- |
| **JOB TITLE** |
| **Information Security Analyst – 12 Months (FTC)** |
| **JOB PURPOSE** |
| The Information Security Analyst will serve as the focal point security and compliance related activities primarily within the Service Management Team (SMT). Your role incorporates advisory, support, assurance, research, development, implementation, testing and reviewing of systems and processes from a security perspective.  You should ensure that we have the right security setup in place to protect ITSO Security management system (ISMS), IT Networks, Data and Services from unauthorized access and exploitation from hackers or malicious attackers.  The role has responsibility for informing users and members about security measures, explaining potential threats, recommending software configuration, and providing security guidance that ensures that ITSO Schemes continue to meet industry security standards.  You would be required to work with the Services and Infrastructure Manager and team members to implement appropriate fixes and solutions. |
| **REPORTS TO** |
| **Services and Infrastructure Manager** |
| **DIRECT REPORTS** |
| **None** |
| **KEY RESPONSIBILITIES** |
| **Security Monitoring & Auditing**   * Plan and coordinate annual penetration testing for all ITSO Services (i.e. ISMS, IT Production, Website and etc). * Review pen testing reports, identify remediation actions, work with service analysts to ensure that agreed recommended actions have been implemented and interim/retesting have been carried out. * Perform validation checks/testing following changes to a service component or as part of a new service delivery. * Plan regular network security checking/scanning and provide remediation actions to ensure our network/systems security baseline is updated always. * Ensure that relevant events alerts are configured to ensure a proactive and prompt response to potential security issues. * Extensive log collection and auditing to detect policy violations such as intrusions and other breaches of security policies (by attackers, staff, 3rd parties with network access, etc.)   **Information Security Management**   * Assisting with the development and implementation of the company’s information security policies, standards and procedures * Documentation of a formalised process for managing security incidents (incident life-cycle, categorisation, priorities, etc.) * Set and approve hardware/software/network/firewall security configurations by collaborating with IT analysts and suppliers. * Ensure that there’s a formal process for logging and tracking all security incidents * Ensure knowledge sharing is in place by creating, maintaining and providing guidance as well as overseeing the implementation of policies. * Initiating, facilitating and promoting activities to foster information security awareness within the company. * Testing and implementation of fixes in response to critical security alerts or issues (i.e.: ‘wannacrypt’ ransomware, Apache Struts vulnerability on the ISMS, virus detections, etc.)   **Security Risk Management**   * Provide documented guidance for configuring anti-virus, malware and security related products (e.g. Avira). * Communicate security issues and general updates and warnings in a manner that be understood by all staff to avoid ambiguity. * Provide security risk analysis with balanced threat assessment based on likelihood, impact and maintain a register of accepted business risk. * Review change requests to ensure that any security risk is identified and managed as part of the change implementation. * Regular access control assessments and adjustment where necessary for firewall rules, staff access rights, admin users, etc. * Continually review and improve upon existing systems by engaging with key business owners to discuss issues/concerns relating to processes, services, and system functions identified during internal audit’s or risk assessments. * Assist in the evaluate security considerations for all new technology projects, provide a security requirements document and advise on best practice following consultation with the project owner. * Lead security management of 3rd party suppliers and partners   **Security Development, research and Training**   * Review of an IT Security policy to reflect current business requirements and standards. * Develop processes and controls in the spirit of ISO27001 * Use internal and external research sources to analyse potential incidents, trends and threats to ITSO.   **Others**   * Facilitation of quarterly ITSO Security Committee meetings |
| **SKILLS, KNOWLEDGE AND EXPERIENCE – ESSENTIAL** |
| * Strong communication skills together with sound judgment when working with sensitive information. * A team player who understands the need to collaboration with involved stakeholders when it comes to security assurance. * A strong background in risk management, auditing and incident impact mitigation * Experience using vulnerability scanning tools such as Nessus * Industry experience with smartcard systems and public transport. * PCI-DSS knowledge also very useful, as well as experience with Linux or Windows |
| **REQUIRED LEVEL OF EDUCATION/AND TECHNICAL CAPABILITIES** |
| * Knowledge of information security architecture, Network protocols, Cloud, Firewalls beneficial * Relevant qualification in Information Security or related IT disciplines |