Job Description – Information Security Engineer

Department	Information Security
Grade	13
Reporting to	Cyber Security Manager
Direct reports (yes or no)	No
WTW Code	AFY637P313

Job Purpose

- To design, implement, maintain, and continually improve security controls and technologies across MIB's environment in partnership with relevant technology teams. The role is responsible for delivering effective, practical security engineering outcomes that reduce risk, strengthen resilience, and support compliance with internal standards and regulatory requirements. The postholder will identify control gaps, support secure technical change, and contribute engineering expertise to the design, integration, and operation of security solutions.

Key accountabilities

- **Security engineering:** Design, implement, configure, and maintain security controls and technologies across MIB's environment to reduce risk and improve resilience.
- Support the integration of security tooling into infrastructure, cloud platforms, end-user computing, and business services in partnership with relevant technology teams.
- **Control improvement and assurance:** Identify security control gaps, weaknesses, and improvement opportunities through review, monitoring, testing, and analysis, and support remediation activity.
- Contribute to the maintenance of security standards, technical procedures, and supporting documentation to ensure controls remain effective, supportable, and aligned to internal and regulatory requirements.
- **Operational security support:** Monitor the effectiveness of implemented controls and support the investigation, containment, and technical remediation of security issues in conjunction with SecOps and other relevant teams.
- Support the ongoing operation, tuning, and optimisation of security technologies to improve detection, protection, and response outcomes.

Key accountabilities

- **Secure technical change:** Provide practical security engineering input to technical change, system implementations, and service improvements to ensure security requirements are addressed during delivery.
- Contribute to change and design review activity where needed, helping ensure solutions meet security standards without taking ownership of broader governance or architectural authority.

Role requirements

Essential

- Demonstrable experience in a security engineering, security operations, or infrastructure security role.
- Hands-on experience implementing, configuring, supporting, and improving security controls and technologies in enterprise environments.
- Good understanding of core security domains such as endpoint protection, identity and access management, vulnerability management, logging and monitoring, email security, and network security.
- Experience supporting secure technical change, troubleshooting security issues, and working with infrastructure, cloud, and application teams to remediate control gaps.
- Working knowledge of security frameworks and standards such as ISO 27001, NIST, and OWASP, and the ability to apply them in a practical delivery context.
- Strong analytical, problem-solving, organisational, and written and verbal communication skills.

Desirable

- Experience working with Microsoft cloud and security technologies, including Azure and related security capabilities.
- Experience with security tooling such as SIEM, EDR, web security, email security, vulnerability management, and related operational platforms.
- Relevant security or vendor certifications, such as CISSP, SC-200, SC-300, AZ-500, or equivalent.
- Experience working in regulated environments and supporting compliance-driven security improvements.