Job Description – Security Operations Analyst

Department	IS, Information Security
Grade	G12
Reporting to	Security Operations Analyst
Direct reports (yes or no)	No
WTW Code	AFY637 P2 12

Job purpose

As a member of the Information Security – Security Operations team (SecOps), you will maintain the confidentiality, availability and integrity of MIB's information and information systems. This will primarily be achieved through identification and mitigation of risk through security systems management and incident management.

- Rapid response, detection, isolation, and remediation of information security incidents.
- Maintain the security technical systems, services, and defenses at MIB.
- To monitor cyber threats and media reports against MIB's security profile to ensure that MIB technical controls are appropriate.
- Maintaining forensic capabilities in the identification of root-cause, containment, and eradication of security threats.
- To provide a focal point within MIB for technical information security expertise.

Key accountabilities

- Maintain the security technical systems, services, and defenses at MIB.
- Rapid response, detection, isolation and remediation of information security incidents.
- Working with problem management teams on mitigation and incident prevention activities.
- Maintaining forensic capabilities in the identification, root-cause, containment and eradication of security threats.
- To monitor cyber threats and media reports against MIB's security profile to ensure that MIB technical controls are appropriate.
- To deliver a vulnerability management service that aligns GRC risk tolerances and business needs.
- To establish and maintain security technical standards, procedures and guidelines.
- To provide IS teams with security focused technical support, training and consultancy to ensure compliance with security standards, policies and legislation.
- Retain a working knowledge of related MIB services areas such as Cloud & end user computing to enable effective liaison with other technical groups and the coherent protection of MIB services.

Key accountabilities

- Produce performance metrics to demonstrate the efficiency and effectiveness of IS and Security Operations controls.
- Develop and operate procedures that counteract potential threats/vulnerabilities.
- Support of the IS Change Management Process ensuring that information security risks are identified and addressed.
- To provide a focal point within MIB for technical information security expertise.
- On Call (out of hours support) ensuring 24/7 security cover of MIB services.

Role requirements

- Demonstrable exposure to cyber incident response.
- Experience of working in an IT Security/IT Operations, or equivalent position.
- Ability to conduct and direct research into threats and vulnerabilities and preventative capabilities.
- Thorough understanding of the cyber threat landscape, significant risks, developments, and directions.
- Extensive technology experience and expertise across a wide range of security technical products and services.
- Think like a hacker – understand the tools and skills used to attack systems to protect MIB against such threats.
- Strong interpersonal skills are essential, as the jobholder must be able to operate effectively at all levels.

One or more of the following qualifications are highly desirable:

- Industry certifications such as CompTIA, SANS, ISC(2).
- MSc Information Security.
- Vendor technology trained (certifications) e.g., SIEM, EDR, IPS, web and email gateway.