Role Profile

Role Title	Level	Team	Function
Security Engineer		IFGL Technology	IT Security

Purpose of the Role
The Security Engineer, reporting into the Head of IT Security, will assist with the translation of the Group's Information Security policies and standards into practical operational procedures. This role holder will work as part of the IT Security Team in areas including the design, implementation and maintenance of robust security measures across network and Cloud environments, ensuring protection against potential threats, adherence to industry standards, and proactive incident response. This will include providing security consultancy services to the Change Team on projects requiring it.

Key Contribution Areas

Measures

Key Contribution Areas	Measures
Provide domain expertise in the operationalisation of IFGL’s Information Security Policies	Collaborate with the Head of IT Security in areas to include: • Ensure continual alignment of Information Security Policies with industry standards, regulatory requirements, and evolving cyber threats. • Develop and communicate an effective strategy for the implementation of Information Security Policies across all departments and systems within the organisation. • Establish mechanisms to regularly monitor and, measure compliance with Information Security Policies, addressing non-compliance issues • Maintain updated documentation, providing easy access to policies, guidelines, and procedures for all staff members.
Ensure adherence with relevant Information Security Frameworks and Certifications	Collaborate with the Head of IT Security to: • Establish a robust mechanism to ensure alignment with relevant Information Security Frameworks (e.g., ISO 27000 series, NIST, etc.), mapping organisational policies and practices to the framework's requirements. • Conduct periodic internal assessments to evaluate adherence to Information Security Frameworks and compliance standards, driving continuous improvement and implement corrective actions based on assessment findings. • Stay updated with industry trends, best practices, regulatory standards and amendments in Information Security Frameworks.
Network and Cloud Security Leadership Lead initiatives to design and implement security solutions for network and Cloud environments	Collaborate with the Head of IT Security to: • Develop strategic plans outlining security objectives and domain roadmaps for network and Cloud environments aligned with organisational goals. • Develop and implement security focused Architecture Building Blocks (ABBs) and Solution Building Blocks (SBBs) in collaboration with the IFGL Architecture team. • Ensure adherence to industry best practices, regulatory standards, and internal security policies across network and Cloud environments. • Develop and implement incident response plans specific to network and Cloud security incidents, outlining clear protocols for detection, containment, and recovery.

Work with External Security Partners	Collaborate with the Head of IT Security to: - Identify and establish partnerships with external security entities, including vendors, consultants, industry groups, or security forums. - Regularly assess the performance and alignment of external security partners with organisational security objectives. - Establish channels for continuous intelligence gathering from external partners regarding emerging threats, vulnerabilities, and best practices. - Foster an environment of knowledge sharing and cooperation to leverage expertise from external entities.
Assess and Assure Security Posture of IFGL's Material IT Suppliers	Collaborate with the Head of IT Security and Head of IT Service to: - Develop a comprehensive framework for assessing the security posture of Material IT Suppliers, outlining assessment criteria, methodologies, and evaluation metrics. - Working with the Head of IT Service, establish mechanisms to verify and validate the compliance of Material IT Suppliers with agreed-upon security standards, contractual obligations, and regulatory requirements. - Conduct thorough assessments to identify security risks associated with Material IT Suppliers, considering factors like data handling, access controls, and compliance. - Implement tools or systems for continuous monitoring of security practices and performance of Material IT Suppliers.
Risk Assessment and Incident Response Conduct risk assessments, analyse vulnerability and penetration testing reports.	Collaborate with the Head of IT Security and Head of Risk to: - Develop a standardised framework for conducting comprehensive risk assessments across the organisation's systems, applications, and infrastructure. - Conduct periodic risk assessments to identify, analyse, and prioritise potential risks and threats to the organisation's assets and operations. - Develop and implement risk mitigation strategies based on the findings from risk assessments, vulnerability testing, and penetration testing reports. - Organise and oversee regular vulnerability assessments and penetration testing activities to identify weaknesses and potential entry points for cyber threats. - Develop and maintain incident response plans aligned with identified risks and potential threats.

Access Management	Collaborate with the Head of IT Security and Head of Service Delivery to: • Develop and maintain a robust Role Based Access Control Framework outlining policies, procedures, and guidelines for managing system and network access. • Ensure that an efficient and consistently applied JML process is in place to manage access rights for employees throughout their lifecycle within the organisation. • Enforce the Principle of Least Privilege across systems and applications, granting users the minimum levels of access necessary to perform their job functions. • Conduct regular access reviews and audits to ensure compliance with access control policies, identifying and addressing any access discrepancies or anomalies.
Provision Information Security training and awareness for colleagues across the Group	Collaborate with the Head of IT Security to: • Develop comprehensive Information Security training programs tailored for different departments and roles across the organisation, using various mediums such as workshops, webinars, online courses, or in-person sessions. • Use feedback to continuously improve training content and delivery methods to enhance their impact. • Implement ongoing awareness campaigns, newsletters, or communication channels to keep staff informed about the latest Information Security threats, trends, and best practices. • Offer expert advice and consultation to project teams within the department regarding network and Cloud security requirements, best practices, and standards.

Functional or Technical Knowledge and Skills Required

- Degree in Computer Science, Information Security, or related field (or equivalent experience).
- Advanced certifications (or working towards such a certification) such as CISSP, CISM, or equivalent are preferred.
- 5+ years in network and / or Cloud security roles, demonstrating progressive responsibility.
- Proven experience in designing and implementing security solutions in network and Cloud environments.
- Extensive experience in IT security, with a focus on Security Operations, Access Management, and Policy Development.
- Strong knowledge of security frameworks, such as NIST and ISO27000 series
- Up-to-date knowledge of emerging security threats, trends, and technologies.
- Expertise in network security protocols, Cloud security solutions (Azure/AWS/GCP), firewalls, intrusion detection systems, VPNs, etc.
- Proficient in vulnerability assessment tools, incident response frameworks, and risk management methodologies.
- Analytical mindset and problem-solving abilities to assess security risks and propose appropriate mitigation strategies.
- A basic understanding for compliance and risk management.

Personal Capabilities Required, e.g. skills, attitude, strengths

- Strong communication, and problem-solving skills.
- Ability to collaborate effectively with cross-functional teams.
- Strong analytical skills to interpret security data and make informed decisions
- Demonstrate an ability to think and reason logically. To adapt to a fast-paced environment and handle multiple priorities effectively.
- Excellent relationship management skills, comfortable in dealing with stakeholders up to Executive and Board level
- Excellent spoken and written communication skills, with the ability to translate complex technical topics into a language that meets the audience's knowledge level

People, Budget and Project Scope

- Reports directly to the Head of IT Security as part of the Technology Department.
- Takes into account the corporate risk framework in relation to risk appetite.