IT Security Architect
Reporting to: IT Security Manager

Main activities and responsibilities:

- Develops and maintains a security architecture process that enables the enterprise to develop and implement security solutions and capabilities that are clearly aligned with business, technology and threat drivers.
- Develops security strategy plans and roadmaps based on sound enterprise architecture practices.
- Develops and maintains security architecture artifacts (e.g., models, templates, standards and procedures) that can be used to leverage security capabilities in projects and operations.
- Determines baseline security configuration standards for operating systems (e.g., OS hardening), network segmentation and identity and access management (IAM).
- Drafts security procedures and standards to be reviewed and approved by IT management.
- Establishes a taxonomy of indicators of compromise (IOCs) and share this detail within IT group, including the IT Security Management, the security operations center (SOC) and IT Operations.
- Tracks developments and changes in the digital business and threat environments to ensure that they are adequately addressed in security strategy plans and architecture artifacts.
- Validates IT infrastructure and other reference architectures for security best practices and recommend changes to enhance security and reduce risks, where applicable.
- Validates security configurations and access to security infrastructure tools, including firewalls, IPSs, Email Security Gateways, Web Security Gateways, WAFs, EDRs and SIEM systems.
- Conducts or facilitate threat modeling of services and applications that tie to the risk and data associated with the service or application.
- Supports the development and implementation IT security controls.
- Reviews security technologies, tools and services, and makes recommendations to the broader IT team for their use, based on risk, financial and operational metrics.
- Liaises with business teams to conduct security assessments of existing and prospective vendors and services:
    - Information Systems used to process critical and strategic business data.
    - Web Applications.
    - Cloud solution providers (IaaS, PaaS, SaaS)
    - Business process outsourcing (BPOs)
    - Managed service providers (MSPs)
- Evaluates the statements of work (SOWs) for these providers to ensure that adequate security protections and controls are in place.
- Liaises with other IT members to share best practices and insights.
- Liaises with the business continuity team to validate security practices for BCP/DR testing and operations when a failover occurs.
- Participates in application and infrastructure projects to provide security-planning and security by design advice.
- Liaises with the internal audit team to review and evaluate the design and operational effectiveness of security-related controls.
- Liaises with important security and risk management stakeholders. Specifically, the security architect may be expected to work collaboratively with individuals or departments, including:
    - IT Security Manager
    - IT Management
    - IT Infrastructure & Operations
    - MSSPs
    - Project Managers
    - Process and System Owners
    - Business Managers.
    - Legal Department
    - Data privacy officer (DPO)

Education:

- Preferable in computer science, information security, cybersecurity.
- Postgraduate, MBA, Master, PhD.
- Fluent English.