Group Information Security & Privacy

Objective

The Group Information Security Policy is designed to support business operations by ensuring a secure and adaptable environment. It focuses on three core security principles:

- **Confidentiality:** Restricts information access and disclosure to authorized individuals and services, ensuring that information is only accessible on a need-to-know and least privileged basis.
- **Integrity:** Ensures that information has not been modified or deleted in an unauthorized and undetected manner, maintaining the accuracy and trustworthiness of the data.
- **Availability:** Provides timely and reliable access to and use of information, ensuring that authorized users can access the information they need when they need it.

By adhering to these principles, the policy aims to support business strategy, customer outcomes, and compliance with legal and regulatory requirements.

Principles and Policy Summary

The policy aims to build and maintain a resilient Information Security Programme for Prudential. It incorporates applicable business and regulatory requirements globally and considers industry best practices to address continuously evolving cybersecurity threats.
In summary, this policy outlines information security control requirements and expectations across all Prudential LBUs and Head offices. It includes:

- **Management direction:** Establishes robust information security governance and assurance, including programme oversight and compliance management.
- **User responsibilities:** Emphasizes protecting Prudential information assets and digital realms through a risk-based approach with defined key performance and risk indicators.
- **Awareness and training:** Provides appropriate information security education to equip users with knowledge to defend against known and unknown threats.
- **Threat intelligence:** Ensures Prudential can anticipate, contain, and mitigate threats to an acceptable risk level.
- **Data classification and handling:** Protects data according to its classification level throughout Prudential.
- **Access control management:** Applies principles of "need to access" and "least privilege" to manage access to corporate systems and information, including privileged access management, access governance, and application authentication/authorization controls.
- **Infrastructure security:** Prevents and mitigates threats from viruses, malware, and worms targeting digital assets.

- **Data protection:** Prevents and mitigates risks of data exfiltration and unauthorized data leakage.
- **Secure application development:** Ensures new systems or modifications to existing systems are adequately protected.
- **External attack surface management:** Conducts security assessments and penetration testing on external-facing assets and technologies.
- **Vulnerability management:** Identifies and remediates vulnerabilities or software weaknesses in a timely manner.
- **Threat detection and incident response:** Monitors and responds to security incidents, ensuring they are detected, triaged, contained, and prevented according to severity and response time.
- **Third-party security management:** Conducts information security due diligence, monitoring, and governance for third parties.
- **Policy management:** Maintains the information security policy to ensure its relevance o the ever-changing threat landscape.