Group Information Security Policy

Objective

The Group Information Security Policy supports the business to deliver on customer outcomes, business strategy, and any applicable legal and regulatory requirements by maintaining a secure and adaptable environment to do business.

The policy has been developed to ensure the confidentiality, integrity, and availability of Information Systems and IT assets (e.g., IT applications, systems, and facilities). Specifically,

- **Confidentiality** – restricts information access and disclosure to authorised and services for authorised purposes on a need-to-know and least privileged basis;
- **Integrity** – ensures that information has not been modified or deleted in an unauthorised and undetected manner; and
- **Availability** – provides timely and reliable access to and use of information.

Principles and Policy Summary

The policy helps to build and maintain a resilient Information Security Programme for Prudential. The policy incorporates not only applicable business and regulatory requirements, where appropriate, across the globe, but also considers industry best practices to address continuously evolving cyber security threats.

In summary, this policy provides directives on information security control requirements and expectations across all Prudential LBUs and Head offices which cover:

- **Management's roles and responsibilities** in establishing and ensuring robust information security governance that includes programme oversight and risk management.
- **Users' responsibilities and participations** in protecting Prudential information assets and digital realms, including the importance of ongoing information security awareness training program for users and acceptable use of assets.
- **Threat intelligence function and capability** that will ensure Prudential will always be able to anticipate, reduce and contain threats.
- **Information classification and handling** to ensure information throughout Prudential is protected in accordance with its classification level.
- **Access control management** to ensure appropriateness of access to corporate systems and information, including privileged access management, authentication credentials management and application access authorisation.
- **Endpoint protection** to defend against malware attacks and data leakage.
- **Secure system development and delivery** to ensure that any new system or modification to existing system will continue be providing adequate protection to data and business functionality.
- **Security assessment and penetration testing** on external facing assets and technologies.
- **Vulnerability management** across all technology assets in order to ensure all attack surfaces exposures are identified and addressed in a timely manner.
- **Security operation monitoring and Incident response handling** capability to ensure security incidents can be prevented, detected and contained.
- **Third party security management** through information security due diligence, monitoring and governance.