LATITUDE FINANCIAL SERVICES AUSTRALIA AND NEW ZEALAND ("LATITUDE")

Information Security Policy

Issued by: Information Security

Approved by: KVDA Board – 30/05/2019

Effective Date: 30/05/2019

Document Owner: Executive General Manager Digital and Technology

Document Contact: General Manager Information Security

Contents

1 Scope

1.1 Applicability

The Information Security Policy ('this 'Policy') applies to all entities within the Latitude Financial Services Group in both Australia and New Zealand ('Latitude' or 'Organisation') and its employees and contractors, and any third-party who have access to Latitude information and associated information systems and facilities.

2 Overview and Purpose

The Information Security Policy sets a clear expectation for the Organisation to ensure that risks relating to information security are managed and that our information is protected from threats, whether internal or external, deliberate or accidental.

The Policy addresses specific focus areas and is further supported by a series of information security standards, guidelines, processes and procedures documents which comprise the Information Security Policy Framework; to provide implementation-level detail for specific operational tasks, requirements and appropriate mitigating controls.

Information Security shall be managed through an Information Security Management System (ISMS). The ISMS shall leverage risk-based decisions informing the use of appropriate controls and safeguards to protect the Organisation.

3 Guiding Principles

Latitude shall implement controls to maintain the Confidentiality, Integrity and Availability of information, systems and facilities while maintaining compliance with legislative, industry, regulatory and contractual requirements.

To achieve this, Latitude has identified a set of core security principles:

- **Confidentiality** - Access to information shall be restricted only to authorised personnel with an explicit entitlement. Sensitive and confidential information shall be handled in accordance with its security classification and privacy consideration
- **Integrity** - Information shall be accurate, complete and free from unauthorised change or usage. Information shall have adequate security to safeguard and to ensure its accuracy, reliability, completeness and authenticity
- **Availability -** Information shall be accessible and usable when it is required. Disaster recovery and business continuity shall be in place to ensure the availability of information, systems, and facilities
- **Compliance -** Access and handling of information assets must comply with all applicable legislation, regulations, policies and contractual obligations requiring information to be available, safeguarded or lawfully used
- **Defence in depth -** Multiple layers and types of controls shall be implemented such that if one control fails, other controls limit the impact of an information security compromise
- **Least privilege** - Users and systems shall have the minimum level of access necessary to perform their defined function
- **Timely detection** - Information Security incidents shall be detected in a timely manner
- **Secure by design -** Security must be incorporated into the design of information and systems
- **Unique identification** - Use of, and access to, information assets is attributable to an individual, hardware or software with the activity logged and monitored
- **Fail securely** - Error handling is designed such that errors do not allow unauthorised access to information assets or other information security compromises
- **Never trust, always identify** - Assume information assets have an unknown and possibly reduced level of information security control
- **Segregation of duties** - Appropriate allocation of roles and responsibilities to reduce potential for a single person to compromise information and systems

- **Assumed breach** - Design detection and response controls based on the assumption that preventive controls have failed

4 Roles & Responsibilities

The following positions and groups have specific information security-related roles and responsibilities for Information Security, including decision-making, approval, oversight, operations and other information security functions:

The Board

Ensure that Latitude maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the Organisation, through the following:

- Information security capability - Consider the sufficiency of information security capability in relation to vulnerabilities and threats; ensure sufficiency of investment to support the information security capability; and review progress with respect to execution of the information security strategy
- Approval of the Information Security Policy
- Implementation of controls - Regularly seek assurance from and, as appropriate, challenge management on reporting regarding the effectiveness of the information security control environment and the overall health of information assets
- Security incident capability - Regularly seek assurance from, and, as appropriate, challenge management on the sufficiency to detect and respond to information security incidents in a timely manner; form a view as to the effectiveness of the security incident capability based on the results of post incident assessments
- Testing control effectiveness - Regularly seek assurance from and, as appropriate, challenge management on the sufficiency of testing coverage across the control environment; form a view as to the effectiveness of the information security controls based on the results of the testing conducted
- Internal audit - Consider the sufficiency of internal audit's coverage, skills, capacity and capabilities with respect to the provision of independent assurance that information security is maintained; form a view as to the effectiveness of information security controls based on audit conclusions; and consider where further assurance, including through expert opinion or other means, is warranted

Executive Committee

- Ensuring the Information Security Policy is effectively communicated and implemented
- Developing and implementing cost effective processes and controls to manage information security risks to meet compliance obligations
- Implementing corrective action to address control deficiencies
- Taking action to assess and, if required, act on escalated information security risk and issues
- Ensuring all information security training is completed and to monitor compliance with training requirements

Management Committees

Information Security risk shall be managed through established corporate governance functions.

General Manager Information Security

- Implementing the Information Security Policy as directed by the Information Security Statement
- Developing, maintaining and executing the information security strategy and program
- Developing, implementing and maintaining the ISMS
- Being kept informed about the current information security condition
- Reporting a high-level summary of the information security condition that highlights key risks and vulnerabilities within the Organisation to the Board and other management committees
- Oversee information security activities aligned to common security functions (such as threat identification/protection, incident response/recovery) to strengthen the Organisation's cyber security defences

This role shall provide the driving force for information security within the Organisation.

Information Owner

- Ensuring that risk assessments for their information assets are completed appropriately, and reviewed on a regular basis
- Accepting the residual risks associated with their information systems
- Monitoring the security condition of their information assets

System Owner

- Ensuring information security requirements have been determined for information systems
- Monitoring and maintaining the security condition of their information systems

Procurement

- Ensuring that relevant information security clauses are included in contracts with third-parties who have; responsibility for managing Latitude information, information systems and facilities; access to Latitude information, information systems and facilities
- Reviewing third-party compliance with their Latitude information security obligations

Employees and third parties

- Complying with Information Security Policy, principles and standards
- Participating in relevant information security training
- Contacting Information Security if they suspect or detect any breaches of policy, material incidents or risks

5 Information Security Policy

The objective of the Information Security Policy is to provide management direction and support for Information Security in accordance with business requirements and relevant laws and regulations.

The Policy shall be approved by management, published and communicated to employees and relevant external parties.

The Policy is based on the international standards and best practices for information security contained in ISO 27001/2, containing 13 domains.

A set of supporting standards shall be established for each domain area, providing implementation details.

6 Organisation of Information Security

Information security shall be managed through the establishment of an Information Security Management System (ISMS) that leverages risk-based decisions informing the use of appropriate controls and safeguards to protect information, systems and facilities.

7 Human Resources Security

Information security shall be considered at all stages of the employment lifecycle, including ongoing information security training and awareness.

8 Asset Management

All assets shall be identified, protected and handled based on information classification, and shall be securely disposed of, or destroyed, when no longer required.

9 Access Control

Access control and user access management shall be applied to all information, information systems and facilities.

10 Cryptography

Appropriate cryptographic controls shall be implemented to protect the confidentiality, authenticity and integrity of information, based on the information classification.

11 Physical and Environmental Security

Physical and environmental controls shall be implemented to protect information, information systems and facilities.

12 Operations Security

The management of production IT: change management, capacity management, malware protection, backup, logging, monitoring, installation, vulnerability management and auditing activities; shall provide adequate protection for information and information systems through operating practices and technology mechanisms.

Information security practices and controls shall be adopted to manage the risks of accessing information when using mobile devices and working from remote locations.

13 Communications Security

Information security controls, including requirements for network security, network segregation, network services, transfer of information and messaging, shall be implemented to protect information in transit from unauthorised parties.

14 System Acquisition, Development and Maintenance

Information security shall be included throughout all phases of the information system acquisition and development lifecycle to reduce or minimise security exposures in software.

15 Supplier Relationships

Information security shall be included in supplier relationships and agreements, based on the information handled by the supplier, to mitigate risks due to the actions of external parties.

16 Information Security Incident Management

Information security incidents shall be identified in a timely manner and managed through a maintained and repeatable process to rapidly contain and recover from incidents.

17 Information Security Aspects of Business Continuity Management

Information security shall be incorporated into business continuity management practices to provide for resilience, redundancy and recovery of information, information systems and facilities in adverse situations.

18 Compliance

Information security controls shall be implemented to comply with relevant legal, statutory, regulatory or contractual obligations relating to information security.

19 Policy Governance

19.1 Review, Renewal and Approval

The Information Security Policy is considered a Tier 1 policy which means that it requires Board approval.

Information Security shall review this Policy at least annually. The Executive General Manager Digital and Technology (policy owner) is responsible for reviewing and approving all non-material changes made to this policy.

19.2 Monitoring and Control

Information Security shall be responsible for identifying any instances of non-compliance (including potential non-compliance) under this Policy. Non-compliance shall be highlighted to the Board.

19.3 Exceptions

Any requests for policy exceptions must be documented in writing and submitted to Information Security for review and approval. Such requests must identify the entity/function/individual requesting the exception, and the nature, timing and duration of the exception. The request must also include corrective action plans to rectify the exception and a proposed timeline for completion of the same.

20 Revision History

Version	Approval Date	Changed By:	Summary of changes
1.0	30 May 2019		Original

Appendix 1 – Terms and Definitions

Principles

Principles are a set of ethics/codes of practice from which the Information Security Policy can be derived. These are the basic information security principles that Latitude shall implement across the Organisation.

Policy

Policy is a set of principles and statements that everyone must comply with. It provides the intent and scope of information security, but not the detail about how information security should be implemented. Standards, Guidelines, Process and Procedures shall support the Information Security Policy.

Standards

Standards are Implementation-level details that help to enforce and support the Information Security Policy.

Processes and Procedures

Processes and Procedures are step-by-step instructions to assist with the implementation of Policy, Standards and Guidelines.

Guidelines

Recommended guidance to support Standards or serve as a reference when no applicable Standard is in place.

Information/Information Asset/Information System

Information and information technology, including software, hardware and data (both soft and hard copy).

Facilities

Latitude offices, premises, sites, data centres that host information, information assets, information systems.

Employees

All Latitude employees and contractors

Appendix 2 – References

- ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management
- APRA CPS 234 Information Security
- APRA Draft PPG 234 Information Security
- Latitude Information Security Statement