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

Acceptable Use Policy

Issued by: Information Security

Approved by: Executive General Manager Digital & Technology – 01/11/2019

Effective Date: 01/11/2019

Document Owner: General Manager Information Security

Document Contact: Information Security

Contents

1 Scope

1.1 Applicability

This Acceptable Use 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 the personnel suppliers who have access to Latitude devices, information, information systems and facilities.

1.2 Effective Date

This Policy is effective from the date of approval.

2 Overview and Purpose

The Information Security Policy defines information security practices and controls related to people, process and technology for protecting Latitude information assets. This enables a consistent and appropriate approach to managing information security risks, minimising the potential impact of information security threats to the Organisation.

This Acceptable Use Policy (the Policy) has been established to define the acceptable behaviour that is expected from employees to comply with the Information Security Policy. Topics covered in this Policy may be included in employee information security training.

3 Requirements

Employees using or having access to Latitude devices, information, information systems and facilities must be aware of the limits existing for their use and will be accountable for their actions.

Employees agree to abide by the terms and conditions of their employment contract and contractual obligations, which include responsibilities for ensuring information security.

Employees who fail to comply with any requirement in this Policy, in the absence of an approved exception, may be considered to be in violation of the Information Security Policy. Failure to comply may result in disciplinary action including possible termination of employment or incur penalties for breaches of supplier agreements.

3.1 General

The use of Latitude devices, information, information systems and facilities must be in compliance with all Latitude policies.

Reasonable personal use of Latitude devices is permitted on the proviso that it is lawful, does not impact productivity, damage Latitude's reputation, or hinder business operations.

All activity on Latitude devices, information systems and facilities is monitored for non-compliance with the Organisation's policies. Employees will have no expectation of privacy relating to their use of the Internet including browsing, email, instant messaging and social media.

Employees must:

- Abide by all laws, regulations (provincial, national and international)
- Conduct themselves in a professional manner that reflects Latitude high ethical standards
- Not bring discredit or embarrassment to Latitude; its employees, suppliers, or competitors
- Not use Latitude resources to achieve personal gain or promote the advancement of personal or political views
- Not use inappropriate language in any communication

- Be sensitive to their surroundings at all times and not reveal business information when having conversations, or when using devices, in public places, open offices and meeting places
- Not share physical access passes or digital credentials (password, authentication token) with others under any circumstances
- Wear identity card when in Latitude facilities
- Complete all relevant information security training
- Report any observed information security incident or suspicious activity, such as:
  - Loss or theft of assets including devices, removable storage media, authentication token
  - Malware
  - Phishing email
  - Policy breach
  - Privacy breach
  - Request for unusual access to confidential or customer information, or for payment
  - Unauthorised access to information
  - Unauthorised access to work area
  - Unauthorised disclosure of information

3.2 Devices and Information

Employees must:

- Only use Latitude devices and information systems which have been pre-authorised
- Only connect authorised devices and network equipment to the Latitude corporate network
- Only use authorised software from authorised sources on Latitude devices and information systems
- Not leave Latitude information unattended at any time. Device screens must be locked, with sensitive information on paper or on removable storage media physically secured when not in use
- Handle information in compliance with Latitude information classification
- Not attempt unauthorised access to work areas or information
- Not remove equipment (other than personally assigned devices) from Latitude facilities without prior authorisation
- Ensure that Latitude devices, information and information systems, when used at home or when remotely working, are not accessible by unauthorised persons (such as family and friends)
- Not deliberately circumvent information security controls on Latitude devices and information systems (such as changing settings or configurations, disabling anti-virus or malware protection, installing unauthorised software)
- Not use network monitoring or security hacking tools unless authorised
- Not attempt to prove suspected security weaknesses. Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the system, resulting in legal liability for the individual performing the testing

3.3 Travel

Employees must:

- Not leave devices or removable storage unattended in public areas
- Not use untrusted or public Wi-Fi connections
- Be aware of people in near proximity when using devices

- Carry devices as hand luggage when travelling by air
- Secure devices out of sight (such as in hand luggage, car boot, hotel room safe)
- Provide international business travel plans to the information security team

3.4 Communications

Employees must:

- Ensure that confidentiality agreements are in place with third parties prior to the exchange of Latitude information
- Not use or reference Latitude email accounts for any non-business purpose
- Not provide information about Latitude's network, information systems, information security, applications, services, and employees to any third-party, without prior authorisation
- Not forward corporate messages (containing internal, confidential or restricted information) to personal email addresses
- Not send unsolicited email messages, including junk mail or other advertising material, to others
- Not forward any spam or phishing email to others
- Not open email attachments received from unknown senders

3.5 Internet

Employees must:

- Not access any Internet-based site that contains information which violates the Latitude Code of Conduct and Latitude values
- Not store Latitude information on a cloud service using a personal account
- Not use the same passwords for Latitude accounts and for personal accounts
- Not represent Latitude unless specifically authorised
- Not share any Latitude information, including photographs and related information about employees, facilities or products
- Not be detrimental to Latitude, its suppliers or competitors
- Not make derogatory or unfounded statements

4 Roles and Responsibilities

The specific information security-related roles and responsibilities for the Acceptable Usage Policy are:

- Employees – Comply with information security policy
- People and Culture – Disciplinary activities
- Information Security – Monitor employee compliance to information security policy

5 Policy Governance

5.1 Review, Renewal and Approval

Information Security (document contact) shall review this Policy at least annually and in conjunction with any associated policy and make any changes that may be required.

The General Manager Information Security (document owner) is responsible for reviewing and approving all changes made to this Policy.

Where an annual review results in no changes being made to the Policy, re-approval by the document owner shall not be required however; the document owner is required to review and re-approve this Policy at least once every three years, even if no changes have been made during that time.

5.2 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.

5.3 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.

6 Revision History

Version	Approval Date	Changed By:	Summary of changes
1.0	01/11/2019		Original

Appendix 1 – Terms and Definitions

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 is implemented. Standards, Guidelines, Processes and Procedures support the Information Security Policy.

Standards

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

Guidelines

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

Processes and Procedures

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

Assets

Physical information technology (hardware) and information-related assets.

Devices

Physical information technology (hardware), such as mobile phones, laptop computers, tablet computers, removable storage media, that is provided to employees to perform their work-related activities.

Employees

Latitude employees and contractors, and the personnel for suppliers who have access to Latitude devices, information, information systems and facilities.

Facilities

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

Information/Information Asset/Information System

Information and information technology, including software, hardware and data.

Appendix 2 – References

- Latitude Information Security Policy
- Latitude Social Media Policy