Information Technology Security Policy

IT Security Policy | Global

Version 2.0 · July 2026 · Confidential — Internal Use

This document is a template intended to be reviewed, tailored and approved by your organisation before use.
Replace all references to “the Company” with your organisation’s name.

Document Control

Document name	Information Technology Security Policy
Document type	IT Security Policy
Jurisdiction	Global
Owner	Chief Information Security Officer
Approved by	Board of Directors
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose

This Information Technology Security Policy is the Board-approved apex document of the Company's information security framework. It states the Board's commitments and requirements for protecting the confidentiality, integrity and availability of the Company's information assets, and gives effect to the expectations of the Company's prudential regulator and to international standards for information security management, principally ISO/IEC 27001:2022, ISO/IEC 27002:2022 and the NIST Cybersecurity Framework 2.0.

The policy establishes: how information security is governed and who is accountable; how information assets are identified and classified; the principles by which security controls are selected, implemented and assured, including where assets are managed by related parties and third parties; how the effectiveness of controls is systematically tested; and how information security incidents are managed and notified to the Company's prudential regulator, data protection authorities and other authorities as applicable law requires.

This policy operates at the level of policy and governance. Technical configuration requirements, control baselines and detailed procedural requirements are set out in [the Company's IT security control standards] and supporting procedures, all of which must be consistent with, and subordinate to, this policy. This policy has been approved by the Board of Directors, which retains ultimate responsibility for the information security of the Company.

2. Scope

This policy applies to:

- all information assets owned by, or operated on behalf of, the Company, in any form (electronic, physical or verbal) and at any location, including assets hosted in cloud services;
- all directors, employees, contractors, secondees and consultants of the Company and its subsidiaries (collectively, staff);
- all related parties and third parties that access, store, process, transmit or otherwise manage the Company's information assets, including material outsourced service providers and their material sub-contractors;
- all stages of the information asset lifecycle, from acquisition or creation through operation to decommissioning and secure destruction; and
- all channels through which information assets are accessed, including corporate networks, remote access, mobile devices and customer-facing digital channels.

Where a related party or third party manages information assets on the Company's behalf, this policy applies to the Company's assessment of, and assurance over, that party's information security capability; the Company remains responsible for the security of its information assets regardless of where they are held. Physical security of premises and personnel security vetting are

addressed in [the Company's physical security and people risk policies] and are within scope of this policy only to the extent they protect information assets.

Jurisdictional application: this policy states international best practice drawn from the standards and frameworks cited in the Regulatory Framework section. The Company must map the requirements of this policy to the law and regulatory requirements of each jurisdiction in which it operates, including prudential rules, data protection law, critical infrastructure legislation and incident reporting obligations. Where the law of an operating jurisdiction imposes a stricter or additional requirement, local law prevails and must be complied with.

3. Definitions

Term	Definition
Information Asset	Information in any form and the technology that stores, processes or transmits it, including data, software, hardware, network infrastructure, cloud services, supporting infrastructure and physical records, whether managed by the Company or by a related party or third-party service provider on its behalf.
Information Security	The preservation of the confidentiality, integrity and availability of information assets and of the systems that store, process or transmit them, achieved through the application of governance, people, process and technology controls, consistent with ISO/IEC 27001:2022.
Information Security Capability	The totality of resources, skills, controls, governance and management arrangements the Company maintains to preserve the confidentiality, integrity and availability of its information assets and to prevent, detect and respond to information security incidents, commensurate with the size and extent of the threats to those assets.
Information security incident	An event, or series of events, that compromises or threatens to compromise the confidentiality, integrity or availability of an information asset, including unauthorised access, disclosure, modification, destruction or denial of service.
Material Information Security Incident	An information security incident that has materially affected, or has the potential to materially affect, financially or non-financially, the Company or the interests of its depositors, customers or other

	stakeholders, and which is therefore notifiable to the Company's prudential regulator or other authorities within the timeframe prescribed by applicable local law.
Control weakness	An information security control deficiency that the Company cannot remediate in a timely manner and which, if material, must be escalated and may be notifiable to the Company's prudential regulator where applicable law so requires.
Information Asset Owner	The executive or senior manager accountable for a defined information asset, group of information assets or record class, including its classification, accuracy, access decisions, risk acceptance, storage, retention, retrieval and eventual destruction.
Classification	The assignment of a criticality and sensitivity rating to an information asset that determines the minimum controls and handling requirements that apply to it.
Criticality	The degree to which the availability and integrity of an information asset is essential to the Company's operations, measured by the impact of its loss or corruption.
Sensitivity	The degree to which unauthorised disclosure of an information asset would cause harm to the Company, its customers or other parties.
Personal Data	Any information relating to an identified or identifiable natural person, whether accurate or not and in whatever form recorded, including identifiers such as name, account and identification numbers, location data, online identifiers and factors specific to that person's identity, consistent with the OECD Privacy Guidelines and applicable data protection law. The terms personal data and personal information are used interchangeably.
Related Party	A person or entity connected to the Company through control, joint control, significant influence or common control, including its subsidiaries and affiliates, other entities within its corporate group, substantial shareholders, its directors and senior managers, their close family members, and any party treated as related under applicable law or accounting

	standards (IAS 24).
Third Party	An external entity outside the Company's corporate group that provides goods or services to the Company under a contractual or other arrangement, or that accesses, stores, processes or transmits the Company's information assets, including suppliers, service providers, intermediaries and their material subcontractors.
Security risk appetite	The nature and level of information security risk the Board is willing to accept in pursuit of the Company's strategic objectives, as articulated in the Board-approved Risk Appetite Statement.
Exception	An approved departure from a requirement of a Company policy, procedure, risk limit, underwriting standard or control, granted on documented merits for a specific transaction, application, customer, process or system and, where applicable, time-limited and recorded with an associated risk acceptance.
Systematic testing	The planned, risk-based programme of testing the design and operating effectiveness of information security controls, including vulnerability assessment and penetration testing.

4. Regulatory Framework

The key legislation, regulations and standards relevant to this document include (as amended from time to time):

Instrument / Standard	Relevance
ISO/IEC 27001:2022 Information security management systems — Requirements	The international standard against which the Company's information security management system, including this policy, its risk assessment and its control selection, is structured and may be certified.
ISO/IEC 27002:2022 Information security controls	The reference catalogue of organisational, people, physical and technological controls from which the Company's Tier 2 security standards are drawn and to which they are mapped.
NIST Cybersecurity Framework 2.0 (2024)	Provides the Govern, Identify, Protect, Detect, Respond and Recover functions

End of preview

This is a preview extract. The complete document continues beyond the pages shown here.

The full document is supplied as a single, fully editable Microsoft Word (.docx) file immediately after purchase — including every remaining section, the definitions, the regulatory framework references and all appendices and templates.

Bracketed prompts such as [30 days] mark the points where your own thresholds, committee names and local regulatory references are inserted.

finance-policies.com