IT 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	IT 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
2. Scope
3. Definitions
4. Regulatory Framework
5. Control Principles
6. Identity and Access Management
7. Authentication and Password Standards
8. Network Security
9. Endpoint and Server Hardening
10. Cryptography and Key Management
11. Email and Web Security
12. Logging, Monitoring and Security Operations
13. Vulnerability Management
14. Secure Development
15. Cloud Security Baseline
16. Backup Security
17. Roles and Responsibilities
18. Exceptions, Breaches and Reporting
Appendix A: Control Mapping to ISO/IEC 27002:2022 and NIST CSF 2.0 (Template)
Policy Administration

1. Purpose

This document sets the mandatory technical security control standards of the Company. It sits directly beneath the enterprise Information Technology Security Policy, which establishes the Company's information security governance, accountability and assurance framework consistent with ISO/IEC 27001:2022 and the NIST Cybersecurity Framework 2.0. That apex policy states what the Board requires; this document specifies, domain by domain, the minimum technical controls that must be implemented and maintained to satisfy those requirements. It does not restate governance content, and where any conflict arises the apex policy prevails.

The controls in this document define the baseline. System owners may implement stronger controls where risk warrants, but may not implement weaker ones without an approved exception under Section 18. Each control is written to be testable: internal and external assurance providers must be able to verify compliance from configuration, tooling output or records.

This document is approved by the Board of Directors, owned by the Chief Information Security Officer (CISO), and reviewed at least annually and on any material change to the threat environment, the Company's technology estate, the international standards it references or applicable regulatory requirements.

2. Scope

This document applies to all information technology assets owned, leased or operated by the Company or operated on its behalf, including: on-premises servers, network infrastructure and end-user devices; cloud infrastructure, platform and software services; mobile devices accessing Company data; operational and corporate applications; and non-production environments. It applies to all employees, contractors, Directors and third parties who administer, develop, configure or access these assets.

Where a material third-party provider operates in-scope assets, the Company must impose equivalent control obligations through contract and verify them under the third-party security assurance requirements of the apex policy and the Outsourcing Policy. Outsourcing an asset does not outsource accountability for its security.

- In scope: production, disaster recovery, development, test and staging environments; corporate and privileged user access; machine-to-machine and service account access.
- Out of scope: physical and environmental security of premises, which this document does not cover and which the Company must address in a separate physical security policy that it is required to produce, and personnel vetting (covered by the IT Staff and Contractor Security Policy), except where this document imposes technical dependencies on them.

2.1 Jurisdictional Application

This document states international best practice anchored to ISO/IEC 27001:2022, ISO/IEC 27002:2022 and NIST CSF 2.0. The Company must map its requirements to the law of each jurisdiction in which it operates — including data protection, critical infrastructure, incident reporting and data-residency law — and where local law or the Company's regulator imposes a stricter requirement, local law prevails.

3. Definitions

Term	Definition
Application Control	A technical control that permits only approved executables, software libraries, scripts and installers to run on a system, and blocks all others by default.
Break-Glass Account	An emergency privileged account held outside normal access-request channels, sealed under dual control and used only when standard privileged access mechanisms are unavailable.
Endpoint Detection and Response (EDR)	Software deployed to workstations and servers that continuously records endpoint activity, detects malicious behaviour and enables remote containment actions such as host isolation.
Hardened Baseline	The approved, security-configured build standard for a class of endpoint, server or service, derived from recognised benchmarks, from which all production instances of that class are deployed.
Immutable Backup	A backup copy that cannot be altered or deleted for a defined retention period, including by an administrator or by ransomware executing with administrative privileges.
Joiner-Mover-Leaver (JML)	The lifecycle process by which user access is provisioned on commencement, adjusted on change of role, and revoked on exit.
Least Privilege	The principle that each identity, including users, service accounts and systems, is granted only the minimum access rights necessary to perform its authorised function, and for no longer than required.
Multi-Factor Authentication (MFA)	Authentication requiring two or more independent factors — something the user knows, has or is — before access is granted; phishing-resistant multi-factor authentication additionally binds the

	authentication to the legitimate service, for example through FIDO2 or smartcard-based methods.
Privileged Access Management (PAM)	The tooling and processes that vault privileged credentials, broker and record privileged sessions, and enforce time-limited, approved elevation of access.
Role-Based Access Control (RBAC)	An access model in which entitlements are grouped into roles aligned to job functions, and users receive access by role assignment rather than by direct entitlement grants.
Secret	A non-human credential such as an API key, service account password, encryption key, certificate private key or connection string.
Security Information and Event Management (SIEM)	The central platform that aggregates and correlates security event logs from mandated sources and generates alerts for triage by the security operations function.
Software Bill of Materials (SBOM)	A structured inventory of the components, libraries and dependencies contained in a software product, maintained so that vulnerable components can be identified and remediated.
Vulnerability	A weakness in a system, configuration or process that could be exploited to compromise the confidentiality, integrity or availability of an information asset.
Zero Trust	A security architecture and design approach in which no user, device or network location is implicitly trusted, and in which every access request is authenticated, authorised, encrypted and continuously evaluated against policy regardless of its origin.

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 Company's information security management system reference standard; this document defines the technical control layer through which Annex A controls are implemented.

ISO/IEC 27002:2022 Information Security Controls	The control catalogue and implementation guidance against which each domain standard in this document is anchored; Appendix A maps sections to 27002 control themes.
NIST Cybersecurity Framework (CSF) 2.0	Provides the Govern, Identify, Protect, Detect, Respond and Recover outcome structure used for the Company's control maturity target profile and for Board reporting on control health.
NIST SP 800-63B Digital Identity Guidelines	Benchmark for the authentication, passphrase and credential lifecycle standards in Section 7, including breach screening and the removal of forced periodic rotation.
CIS Critical Security Controls v8.1 and CIS Benchmarks	Source of prioritised safeguards and the configuration hardening baselines mandated for endpoints, servers, network devices and cloud services.
BCBS Principles for Operational Resilience (2021) and Principles for the Sound Management of Operational Risk	Prudential expectations that information and communication technology risk, including cyber risk, is controlled commensurately with the criticality of the services it supports.
ISO 22301:2019 Business Continuity Management Systems	Backup, restoration testing and recovery controls in Section 16 must satisfy the recovery objectives set under the Company's business continuity management system.
OECD Privacy Guidelines and the EU General Data Protection Regulation (as a reference model)	Encryption, access control, logging, data-masking and breach-handling controls in this document protect personal data and support breach notification obligations under applicable local law.

5. Control Principles

All technical controls must be designed and operated in accordance with the following principles. These principles govern interpretation wherever a specific standard is silent.

- Defence in depth: no single control failure may result in compromise of a critical information asset.
- Least privilege and need-to-know for every human and non-human identity.
- Secure by default: new systems must be deployed from hardened baselines with insecure services and default credentials removed before production use.
- Zero trust orientation: authentication and authorisation must not rely on network location alone.

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