IT Staff and Contractor 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 Staff and Contractor Security Policy
Document type	IT Security Policy
Jurisdiction	Global
Owner	Chief Information Security Officer
Approved by	Chief Executive Officer
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose

This Policy establishes the security obligations of the people who work for and with the Company. Technology and process controls cannot protect the Company's information assets unless the employees, contractors and third-party personnel who use those assets are trustworthy, competent and vigilant. This Policy therefore addresses the people dimension of information security across the full engagement lifecycle: before engagement, at onboarding, during service, on role change and at exit.

The Policy gives effect to the people controls of ISO/IEC 27001:2022 and ISO/IEC 27002:2022, to the identity, access and workforce-awareness outcomes of the NIST Cybersecurity Framework 2.0, and to the expectations of the Company's prudential regulator that the Company maintain an information security capability commensurate with the threats to its information assets, including threats arising from the actions of its own workforce and of third parties with access to those assets.

This Policy has been approved by the Chief Executive Officer on the recommendation of the Chief Information Security Officer (CISO), who owns the Policy and is accountable for its maintenance and effectiveness. It forms part of the Company's information security framework and must be read together with the Information Technology Security Policy (which establishes the Company's information security governance and its data classification scheme), the IT Security Policy (which sets the technical control standards supporting this Policy), the Remote Working and Working From Home Policy and the Code of Conduct.

2. Scope

This Policy applies to the Company and each of its subsidiaries, and to all personnel: permanent and fixed-term employees, directors when using Company systems, secondees, contractors (whether engaged directly or through an agency), consultants, temporary staff, and the personnel of vendors and service providers who are granted access to Company information assets, systems or premises.

It applies to all Company information assets regardless of location or ownership of the device used to access them, including Company-issued equipment, approved personal devices, network services, cloud services procured by the Company, email and collaboration platforms, and physical records. It applies wherever work is performed, including Company premises, remote locations and travel.

- Obligations expressed as applying to "personnel" bind employees, contractors and third-party personnel equally unless expressly stated otherwise.
- Organisational-level security requirements for vendor firms (due diligence, contractual security schedules, assurance) are governed by the Third-Party Risk Management Policy; this Policy governs the individual people supplied under those arrangements.

- Customers and members of the public are outside the scope of this Policy.

Jurisdictional application. This Policy states international best practice, anchored to the frameworks listed in the Regulatory Framework section. The Company must map the requirements of this Policy to the law of each jurisdiction in which it operates — in particular employment, background-check, workplace surveillance and data protection law — and where local law imposes a stricter or conflicting requirement, local law prevails.

3. Definitions

Term	Definition
Personnel	All individuals performing work for or on behalf of the Company, including permanent and fixed-term employees, contractors, secondees, temporary staff and third-party personnel with access to Company information assets.
Contractor	An individual engaged to provide services to the Company under a contract for services, whether directly or through an agency, personal services entity or service provider, and who is not an employee of the Company.
Third-Party Personnel	Employees or subcontractors of a vendor or service provider who are granted access to Company systems, premises or information in the course of delivering services to the Company.
Sponsor	The Company manager, at [manager level or above], accountable for a contractor or other third-party individual engaged by the Company, including for the appropriateness and continuing currency of that individual's access to Company systems and information.
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.
Privileged Access	Access rights that exceed those granted to a standard user, including administrative rights over systems, networks, databases, security controls or cloud tenancies, break-glass and emergency accounts, and the ability to access bulk customer data.

Sensitive Role	A role designated by the Company as requiring enhanced screening because it involves privileged access, access to bulk customer or payment data, security administration, or accountability under the senior manager accountability regime applicable in the Company's jurisdiction(s). Designated sensitive roles are listed in [the Sensitive Roles Register maintained by the CISO].
Screening	Pre-engagement verification of a candidate's identity, right to work, criminal history where lawful, qualifications and references, proportionate to the risk and access level of the role and conducted in accordance with applicable local law.
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.
Approved Tools Register	The register maintained by [the CISO / IT function] of software, cloud services and artificial intelligence tools authorised for use with Company information, located at [location/link].
Removable Media	Portable storage devices including USB drives, external hard drives, optical media and memory cards.
Security Incident	An event that compromises, or could compromise, the confidentiality, integrity or availability of Company information assets, including phishing, malware, unauthorised access, and loss or theft of devices or data.
Phishing	An attempt to deceive personnel, by email, SMS, telephone, messaging or other means, into disclosing credentials or information, transferring funds, or executing malicious content.
Confidentiality Agreement	A confidentiality and non-disclosure agreement executed by a contractor or third-party individual before access to Company information is granted, imposing obligations equivalent to those of employees and surviving the end of the engagement.

Clean Desk	The practice of securing all physical documents, media and authentication devices when a workspace is unattended and at the end of each working day.
Acceptable Use	Use of Company systems and information that complies with this Policy, is lawful, and is consistent with the individual's role and the Company's interests.

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	Requires the Company's information security management system to address human resource security across the employment lifecycle, including Annex A people controls.
ISO/IEC 27002:2022 Information security controls	Provides the implementation guidance for the people controls this Policy operationalises: screening (6.1), terms of employment (6.2), awareness and training (6.3), disciplinary process (6.4), responsibilities after termination (6.5) and confidentiality agreements (6.6).
NIST Cybersecurity Framework 2.0	Informs the Company's identity management, authentication and access control lifecycle (PR.AA), awareness and training outcomes (PR.AT) and governance of workforce cyber risk (GV).
BCBS Principles for Operational Resilience (2021)	Requires management of risks to critical operations arising from people and third-party dependencies, including the personnel of service providers with access to the Company's systems.
BCBS Principles for the Sound Management of Operational Risk (2021)	Establishes expectations for controls over people-related operational risk, including screening, segregation of duties, access management and monitoring.
OECD Privacy Guidelines and the GDPR (as a reference model)	Set the standards applied to the collection, use and retention of personal information obtained through screening and workplace monitoring under this Policy.
UN Security Council sanctions regimes (and applicable autonomous regimes, e.g. OFAC / EU / UK, as examples)	Basis for sanctions screening of candidates for sensitive roles against lists applicable to the Company.

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