Telephone, Mobile and Internet Policy

IT 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	Telephone, Mobile and Internet Policy
Document type	IT Policy
Jurisdiction	Global
Owner	Chief Information 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 sets out the rules governing the issuance, use, management, monitoring and decommissioning of the Company's telephone, mobile, internet, messaging and collaboration facilities. It exists to ensure that Communications Facilities support the efficient conduct of the Company's business, that the information they carry is protected under the Company's information security management system, and that Business Communications are captured and retained so that they can be supervised, reconstructed and produced to a regulator, court, auditor or customer.

Communications Facilities present distinct risks to a regulated financial institution: customer information travels on endpoints that leave Company premises and cross borders; business conducted on unmonitored personal channels destroys the Company's ability to evidence what was said or agreed; telephony and archiving providers are dependencies on which critical operations rely; and misuse creates conduct, privacy, legal and cost exposure. This Policy addresses each risk with operable controls, defined approval points and measurable timeframes.

The controls in this Policy are designed to satisfy ISO/IEC 27001:2022 and 27002:2022, NIST SP 800-124 Rev. 2 and NIST Cybersecurity Framework 2.0, together with prudential expectations for operational risk and resilience.

This Policy has been approved by the Chief Executive Officer and is owned by the Chief Information Officer, who is accountable for its implementation and for the platforms and registers it requires. It must be read with the Information Technology Security Policy, the Privacy Policy, the Document Retention Policy and the Code of Conduct. Terms in square brackets must be completed by the Company.

2. Scope

This Policy applies to all Workers of the Company, its subsidiaries and branches, wherever located and at all times of day, including use outside business hours, while working remotely and while travelling. It binds every Worker who uses Communications Facilities regardless of employment status, location or reporting line.

It covers all Company-issued desk telephones, softphones, mobile telephones, tablets, mobile broadband devices, SIM and eSIM services, internet access, email, instant messaging, collaboration, voice and video conferencing platforms, contact centre telephony, and any personally owned device used under a BYOD arrangement. It applies to personal devices, accounts and numbers only to the extent they are used, or proposed to be used, for Business Communications or to access Company information.

Where a third party operates Communications Facilities on the Company's behalf — carriers, collaboration platforms, UEM/MDM operators, call-recording and archiving vendors and outsourced contact centres — the Company must impose

equivalent control obligations by contract and verify them under the Outsourcing Policy. Outsourcing a channel does not transfer accountability for the security, capture or lawful use of the communications it carries.

- In scope: all Company-issued and BYOD endpoints; all voice, message and internet channels used for Company business; and the archives, recordings and logs those channels generate.
- Out of scope: the security architecture of Company networks and applications generally (Information Technology Security Policy); public communications and marketing content standards (Corporate Communications and Social Media policies); and the handling of personal data generally (Privacy Policy). Where this Policy overlaps, the more stringent requirement prevails.

2.1 Jurisdictional application

This document states international best practice anchored to ISO/IEC 27001:2022, ISO/IEC 27002:2022, NIST SP 800-124 Rev. 2 and NIST CSF 2.0. The Company must map every requirement to the law of each jurisdiction in which it operates — in particular employment and works-council law, employee monitoring and communications interception law, consent requirements for call recording, data protection and data-residency law, financial services record-keeping law, and breach notification law. Where local law, a collective agreement or the Company's regulator imposes a stricter or additional requirement, that requirement prevails and must be reflected in local implementing procedures. Where local law prohibits a control required here, the Chief Information Officer must record the conflict, obtain legal advice and approve a documented compensating control.

3. Definitions

Term	Definition
Approved Channel	A communications platform or service assessed and approved by the Chief Information Officer and listed with the status "Approved" in the Approved Communication Channels Register (Appendix C).
Business Communication	Any communication, in any medium, relating to the Company's business, products, services, customers, counterparties or Workers, including any communication that creates, evidences, instructs or varies a business decision, transaction, order, advice or customer interaction.
BYOD	Bring Your Own Device — an arrangement under which a Worker uses a personally owned device to access Company systems, data or communications services, subject to the conditions in this

	Policy.
Communications Facilities	All telephony, mobile devices, SIM and data services, internet access, email, messaging, collaboration and conferencing services provided, paid for or approved by the Company, together with the networks, archives and management platforms supporting them.
Containerisation	A control that separates Company applications and data on a device into an encrypted, centrally managed workspace, logically isolated from personal content and able to be managed or erased independently of it.
Cost Centre Owner	The manager accountable for the budget against which a device or service is charged, who approves issuance and is responsible for usage costs in that cost centre.
Designated Recorded Line	A telephone line, queue or channel designated by the Chief Risk Officer as supporting activities for which call recording is required, including regulated advice, order taking, customer instructions and complaints handling.
Elevated-Risk Travel Destination	A country or territory listed by the Chief Information Security Officer as presenting elevated risk of device compromise, interception, coercion or lawful seizure. This is a device-security classification, distinct from any money-laundering or sanctions classification.
Jailbroken or Rooted Device	A device on which manufacturer or operating-system security restrictions have been removed, bypassed or disabled, permitting unauthorised software installation or privileged system access.
Legal Hold	A written direction, ordinarily issued by the General Counsel, suspending the routine destruction, deletion, alteration or overwriting of specified records, communications and data that are, or may reasonably become, relevant to litigation, a dispute, an investigation, an audit or a regulatory or supervisory request.
Limited Personal Use	Occasional, brief personal use of Communications Facilities that does not interfere with duties, does not incur material cost to the Company, and

	complies with all conduct requirements of this Policy.
Loan Device	A temporary, minimally configured device issued by IT for travel to an Elevated-Risk Travel Destination or other defined short-term purposes, wiped and rebuilt on return.
Off-Channel Communication	A Business Communication conducted on any channel other than an Approved Channel, including personal messaging applications, personal email, personal voice or video services, and ephemeral or auto-deleting messaging features.
UEM/MDM	Unified Endpoint Management or Mobile Device Management — the Company's platform for enrolling, configuring, monitoring, securing and, where necessary, erasing devices that access Company information.
Remote Wipe	Remote erasure of data from a device via UEM/MDM — full-device erasure for Company-issued devices, or erasure of the work container only for BYOD devices.
Workforce Monitoring	Monitoring of Workers' use of Communications Facilities, including call, message, internet and device-compliance monitoring, conducted in accordance with this Policy and applicable employee monitoring, data protection and interception law.
Worker	Any person who carries out work for the Company or a subsidiary, including directors, employees, secondees, contractors, subcontractors, consultants, agency, temporary and labour hire personnel, interns, apprentices and volunteers.

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; the device, channel and monitoring controls in this Policy are risk treatments within its scope and Statement of

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