ELEVATE
SOLUTIONS

POLICY · BUSINESS & INDUSTRY

Remote Work Security Policy

Hybrid & distributed teams

Security requirements for remote and hybrid employees — device, network, data handling, incident reporting. Ready to adopt: replace the bracketed placeholders, set your defaults, and circulate for signature.

Purpose, scope, and the equipment baseline

This policy is written to be adopted as-is. Square brackets mark the decisions [Company] must make — timeouts, reporting windows, named roles. Every bracketed value below is a workable default, not a placeholder to delete. Tighten them where your regulator, clients, or carrier require it.

FIELD	ENTRY
Policy owner	[Title — e.g., IT Manager or Compliance Officer]
Effective date	[Date]
Version	[1.0]
Review cycle	Annual, and after any material incident or regulatory change

Article 1 — Purpose

1.1 This policy defines the minimum security requirements for any employee, contractor, or temporary worker of [Company] who performs work outside [Company] office locations, whether occasionally, on a hybrid schedule, or full-time.

1.2 The intent is to keep [Company] data — including client, patient, and financial records — protected to the same standard outside the office as inside it.

1.3 The human element is involved in 60% of breaches. Verizon DBIR 2025 This policy exists to make the secure choice the default choice, not to assign blame.

Article 2 — Scope

2.1 This policy applies to all remote and hybrid work performed for [Company], on any device that accesses [Company] systems, email, or data, regardless of who owns the device.

2.2 "Regulated data" in this policy means any data subject to legal, contractual, or regulatory protection, including but not limited to: client files and privileged communications, protected health information (PHI), nonpublic personal financial information, and personnel records.

2.3 Where a client engagement letter, regulator, or insurance policy imposes a stricter requirement than this policy, the stricter requirement controls.

2.4 Exceptions to any clause require written approval from [Policy owner] before the fact, with a documented expiration date. Verbal or after-the-fact exceptions are not valid.

Article 3 — Device requirements

3.1 Remote work is performed on a [Company]-managed device. Personally owned devices (BYOD) may be used only if enrolled in [Company]'s mobile application management (MAM) or device management (MDM) tooling, and only for the applications that tooling protects.

3.2 Full-disk encryption is enabled on every device used for [Company] work: BitLocker on Windows, FileVault on macOS, and default device encryption on iOS/Android. Devices that cannot encrypt at rest are not used for [Company] work.

3.3 Screens lock automatically after no more than [10] minutes of inactivity, and employees lock the screen manually whenever stepping away. Unlock requires a password, PIN of at least [6] digits, or biometric.

3.4 Operating system and application security updates are installed within [14] days of release. Devices that defer updates beyond this window may be blocked from [Company] systems until current.

3.5 [Company]'s endpoint detection and response (EDR) agent is installed, running, and reporting on every managed device. Employees do not disable, pause, or uninstall security tooling for any reason.

3.6 Employees do not hold local administrator rights on managed devices unless granted a documented exception under clause 2.4. Software is installed only from [Company]-approved sources.

3.7 Jailbroken or rooted devices, and devices running operating systems past end-of-support, are prohibited from accessing [Company] systems.

3.8 Removable media (USB drives, external disks) are not used for regulated data unless [Company]-issued and encrypted.

> **ADOPTION NOTE**
>
> Clauses 3.1–3.5 are the ones auditors and cyber-insurance applications ask about most often. If you adopt nothing else verbatim, adopt these five — and make sure your management tooling can actually prove compliance with each one on demand.

Article 4 — Home network requirements

4.1 The home router's administrative password has been changed from the factory default, and remote administration is disabled.

4.2 Home Wi-Fi uses WPA2 or WPA3 encryption with a unique passphrase. WEP and open (unencrypted) networks are prohibited for [Company] work.

4.3 Router firmware is kept current. If the router no longer receives manufacturer updates, the employee notifies [IT contact] for replacement guidance.

4.4 Public Wi-Fi (hotels, cafés, airports, co-working spaces) is not used to access regulated data unless the [Company] VPN is connected first. When in doubt, use a personal phone hotspot instead.

4.5 Household members do not use [Company] devices, and [Company] work is not performed under a shared or family account. Work accounts and personal accounts are kept separate on every device.

4.6 Where the router supports it, employees are encouraged to place smart-home and entertainment devices on a separate guest network from the device used for work.

02 — DATA HANDLING & STORAGE

Where data lives, prints, and appears on screen

Article 5 — Approved storage locations

5.1 [Company] data is created, edited, and stored only in approved locations: [list — e.g., the document management system, SharePoint/OneDrive under the company tenant, and the practice management system]. No other location is approved by default.

5.2 Personal cloud storage (personal Google Drive, Dropbox, iCloud), personal email accounts, and personal messaging apps are never used to store, send, or "temporarily park" [Company] data — including forwarding work email to a personal address.

5.3 Regulated data is not stored on personal devices. The only exception is data held inside a [Company]-managed container (per clause 3.1), which [Company] can wipe remotely without touching personal content.

5.4 Local copies on managed devices are kept to the minimum needed for the task and synced back to the approved location the same business day. Desktops and downloads folders are not long-term storage.

5.5 Data is shared externally only through [approved sharing method — e.g., expiring secure links from the document management system], never as unprotected attachments containing regulated data.

Article 6 — Printing and physical documents

6.1 Printing of regulated data at home is [prohibited / permitted only when a task cannot be completed on screen — select one]. If permitted, printed regulated material is logged or kept to the minimum pages necessary.

6.2 Printed [Company] material is stored out of sight in a locked drawer or cabinet when not in active use, and is never left in vehicles, shared spaces, or household recycling.

6.3 Printed regulated material is destroyed with a cross-cut shredder when no longer needed, or returned to the office for secure destruction within [10] business days. Tearing and discarding is not destruction.

6.4 Home printers used for [Company] work are connected to the home network the employee controls — never to a public or landlord-managed network — and stored print jobs are cleared.

Article 7 — Screen privacy and the workspace

7.1 In shared households, co-working spaces, and public places, screens displaying regulated data are positioned so they cannot be read by others. A privacy filter is required for regular work in public or shared spaces.

7.2 Work calls discussing regulated matters are taken where they cannot be overheard — not in open cafés, transit, or shared rooms within earshot of others.

7.3 Voice assistants and always-listening smart speakers are moved out of, or muted in, the room where confidential calls take place, where practical.

7.4 Devices are locked (clause 3.3) whenever the employee leaves the workspace, even at home, even briefly.

Article 8 — Video call hygiene

8.1 Video calls involving client or regulated matters use [Company]-approved platforms only: [list — e.g., Teams, Zoom under the company account].

8.2 Backgrounds are checked before joining: no visible case files, whiteboards, sticky notes with credentials, or other client-identifying material on camera. A blurred or virtual background is acceptable and encouraged.

8.3 When sharing a screen, employees share a specific window or application — not the full desktop — and close email, chat, and unrelated client files first. Notification banners are silenced (Focus Assist / Do Not Disturb) before any external screenshare.

8.4 Meetings are recorded only with the knowledge of participants and only where [Company] policy and applicable law permit. Recordings are stored in approved locations per clause 5.1, never on personal devices.

8.5 Meeting links for external calls use waiting rooms or lobby admission so uninvited parties cannot join unnoticed.

> **WHY THE STORAGE RULES ARE STRICT**
>
> Third-party involvement appeared in 30% of breaches — double the prior year. Verizon DBIR 2025 Every personal cloud account and consumer app holding firm data is an unvetted third party. Keeping data in approved locations is what makes clauses 9.1–9.3 workable: you cannot wipe, audit, or report on data you cannot locate.

03 — INCIDENT REPORTING & TRAVEL

When something goes wrong, and when you leave home

Article 9 — Incident reporting

9.1 A lost or stolen device that accesses [Company] systems — including personal phones enrolled under clause 3.1 — is reported to [IT contact / phone / email] within [4] hours of discovery, at any hour, any day. Do not wait for business hours.

9.2 A suspected phishing message, account compromise, malware alert, or unexpected MFA prompt is reported immediately upon noticing it. Over 90% of successful cyber-attacks start with a phishing email, CISA and the minutes after a click matter most.

9.3 If an employee clicked a link, opened an attachment, or entered credentials before realizing something was wrong, they say so plainly in the report. Reporting an incident in good faith — including one's own mistake — will not by itself result in discipline. Concealing one will (clause 11.2).

9.4 After reporting, the employee follows instructions from [IT contact]. Employees do not attempt self-remediation: no deleting emails, running cleanup tools, wiping devices, or resetting accounts unless instructed, because doing so can destroy evidence needed for legal, insurance, and breach-notification obligations.

9.5 Suspected exposure of regulated data is escalated by [IT contact] to [Compliance Officer / counsel] the same business day, so that regulatory and client notification clocks are assessed on time.

241 days	$3.61M vs $5.49M	60%
Mean time to identify and contain a breach IBM Cost of a Data Breach Report 2025	Average cost when contained under 200 days vs over IBM Cost of a Data Breach Report 2025	Breaches involving the human element Verizon DBIR 2025

Fast reporting is the single cheapest control in this document. The clauses above only work if employees believe clause 9.3.

Article 10 — Travel

10.1 Devices used for [Company] work remain in the employee's physical custody or in a locked, non-obvious location (hotel safe, locked luggage) at all times while traveling. Devices are never left visible in vehicles or checked in luggage.

10.2 Hotel, airport, and conference Wi-Fi is treated as public Wi-Fi: the [Company] VPN is connected before any [Company] system is accessed (clause 4.4).

10.3 Public USB charging ports and borrowed cables are avoided; employees travel with their own charger and a power-only adapter if needed.

10.4 International travel with a [Company] device, or any intent to work internationally, is reported to [IT contact] at least [10] business days before departure. [Company] may issue a loaner device with minimal

data for the trip, restrict account access by region, or both.

10.5 Border agents in some jurisdictions may lawfully demand device access. Employees comply with lawful orders, do not obstruct inspection, and report any border inspection, confiscation, or out-of-sight handling of a device to [IT contact] within [24] hours. Credentials entered or exposed during inspection are reset on arrival.

10.6 For travel to destinations [Company] designates higher-risk, regulated data is not carried on the device; the employee works through remote sessions only, on a loaner device issued for the trip.

Article 11 — Enforcement

11.1 Compliance with this policy is a condition of remote work privileges and, where stated in employment terms, of employment. [Company] may verify compliance through device management reporting, access logs, and periodic spot checks.

11.2 Violations may result in suspension of remote access, removal of remote work privileges, and disciplinary action up to and including termination, consistent with [Company]'s disciplinary procedures and applicable law. Concealing an incident or knowingly circumventing a control is treated as a serious violation.

11.3 [Company] may immediately suspend or wipe access for any device that presents an active risk, without prior notice, to contain a suspected incident. Personal content in a managed container is not accessed during such actions except as required by law.

11.4 This policy is reviewed at least annually by [Policy owner] and reissued for acknowledgment when materially changed.

Article 12 — Acknowledgment

12.1 I have read and understood the [Company] Remote Work Security Policy, version [1.0]. I agree to follow it, and I understand that I should direct questions to [Policy owner] before — not after — acting outside it.

Employee name (print) _____

Employee signature _____

Date _____

Department / role _____

Received by (manager or HR) _____

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io