**Cybersecurity Templates**

**Mobile Devices & Remote Work Policy**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Mobile Devices & Remote Work Policy** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy ID:** |  | **Owner:** |  |
| **Approved by:** |  | **Effective date:** |  |

Contents

[Mobile Devices & Remote Work Policy 4](#_Toc207120402)

[1. Purpose 4](#_Toc207120403)

[2. Scope 4](#_Toc207120404)

[3. Definitions (selected) 4](#_Toc207120405)

[4. Roles & Responsibilities 4](#_Toc207120406)

[5. Eligibility & Approvals 5](#_Toc207120407)

[6. Remote Work Standards 5](#_Toc207120408)

[6.1 Work Hours & Communication 5](#_Toc207120409)

[6.2 Workspace & Safety 5](#_Toc207120410)

[6.3 Physical Security 5](#_Toc207120411)

[6.4 Network & Connectivity 5](#_Toc207120412)

[7. Mobile Device Governance 6](#_Toc207120413)

[7.1 Enrollment & Ownership Models 6](#_Toc207120414)

[7.2 Minimum Security Baseline (MSB) 6](#_Toc207120415)

[7.3 Acceptable Use 6](#_Toc207120416)

[7.4 Data Handling 6](#_Toc207120417)

[8. Information Security Requirements 7](#_Toc207120418)

[9. Equipment, Support & Expenses 7](#_Toc207120419)

[10. Legal & Compliance 7](#_Toc207120420)

[11. Privacy & Monitoring 7](#_Toc207120421)

[12. Driving & Safety 8](#_Toc207120422)

[13. Insurance & Liability 8](#_Toc207120423)

[14. Compliance & Enforcement 8](#_Toc207120424)

[15. Version Control 8](#_Toc207120425)

[Appendices (Templates & Checklists) 8](#_Toc207120426)

[Appendix A: Remote Work Agreement (one‑page) 8](#_Toc207120427)

[Appendix B: Device Enrollment & Minimum Security Checklist 9](#_Toc207120428)

[Appendix C: BYOD Terms (employee attestation) 9](#_Toc207120429)

[Appendix D: Home Workspace Self‑Assessment (condensed) 9](#_Toc207120430)

[Appendix E: Mobile Device Acceptable Use (quick rules poster) 10](#_Toc207120431)

[Appendix F: Glossary & References 10](#_Toc207120432)

# Mobile Devices & Remote Work Policy

# 1. Purpose

Establish consistent, risk-based rules for remote work and mobile device use (both company-owned and Bring Your Own Device, or BYOD) to safeguard the confidentiality, integrity, and availability of [Company] information, while enabling flexible work arrangements.

# 2. Scope

Covers work performed away from a [Company] site (e.g., home, client site, public space, travel) and any device that can store or access company data (laptops, smartphones, tablets, wearables, removable media). Includes contractors/third parties where contractually required.

# 3. Definitions (selected)

* **BYOD:** Personally owned device authorized to access [Company] resources.
* **COPE:** Company-owned, personally enabled device.
* **EMM/MDM:** Enterprise Mobility/Device Management.
* **Restricted Data:** Highest sensitivity classification as per Information Classification Standard.
* **Secure Network:** Company VPN or trusted corporate network.

# 4. Roles & Responsibilities

|  |  |
| --- | --- |
| **Role** | **Key responsibilities** |
| **Policy Owner** | Maintain policy, coordinate annual review, and approve exceptions. |
| **Managers** | Approve remote work, ensure team compliance, and monitor outcomes. |
| **IT/Security** | Operate MDM/EMM, enforce security baselines, and support incidents. |
| **HR/Legal** | Maintain agreements, address employment & local law considerations. |

|  |  |
| --- | --- |
| Employees/Contractors | Follow this policy, protect devices/data, and report incidents. |

# 5. Eligibility & Approvals

* Remote work is a privilege based on job suitability, performance, and risk.
* Approval required via **Remote Work Agreement** (Appendix A) and **Device Enrollment** (Appendix B).
* Trial periods (e.g., 60–90 days) may be used to validate productivity, security, and ergonomics.
* [Company] may revoke or modify arrangements at any time for business or security reasons.

# 6. Remote Work Standards

## 6.1 Work Hours & Communication

* Work hours, response time SLAs, and on-site attendance expectations are documented in the Remote Work Agreement.
* Employees must be reachable via approved channels during scheduled hours.
* Non-exempt employees record time using [System]; overtime requires prior approval.

## 6.2 Workspace & Safety

* Maintain a dedicated, safe, and ergonomic workspace with adequate privacy and ventilation.
* Complete **Home Workspace Self‑Assessment** (Appendix D) before remote work begins and after material changes.
* Prohibit in-home meetings with clients or colleagues unless explicitly authorized.
* Ensure family/roommates cannot view or access company information.

## 6.3 Physical Security

* Do not leave devices or documents unattended in public or vehicles.
* Use privacy screens in public; position screens to prevent shoulder‑surfing.
* Lock devices when unattended; store paper records in locked containers.

## 6.4 Network & Connectivity

* Use Company VPN for all remote network access.
* Public Wi‑Fi permitted only with VPN and verified SSIDs; avoid captive portals that block VPN.
* Prohibit ad‑hoc tethering/hotspots without security controls.

# 7. Mobile Device Governance

## 7.1 Enrollment & Ownership Models

* **Company‑Owned (COPE):** Must be enrolled in MDM before use.
* **BYOD:** Allowed for approved platforms after attesting to BYOD Terms (Appendix C) and enrolling in MDM.
* Unauthorized devices are **blocked** from corporate resources.

## 7.2 Minimum Security Baseline (MSB)

|  |  |
| --- | --- |
| **Control** | **Requirement** |
| **Supported OS** | iOS/iPadOS [current − 2], Android [current − 2, Google Play services], Windows/macOS [current − 1]. |
| **Patch currency** | OS and app updates are applied within 14 days of release (with critical updates applied within 7 days). |
| **Device lock** | Auto‑lock ≤ 5 minutes; password/passcode required; biometrics allowed with passcode fallback. |
| **Encryption** | Full‑disk/device encryption enabled. |
| **MDM posture** | Device compliant with MDM checks (jailbreak/root detection, secure boot, disk encryption, screen lock). |
| **Malware protection** | Enabled where applicable (e.g., Windows/macOS endpoint protection). |
| **Data separation** | Company workspace/app container; copy/paste & share restricted per classification. |
| **Backups** | Only company-approved encrypted backups are permitted; personal cloud backups for corporate data are prohibited. |
| **Lost mode** | Remote lock/wipe enabled; user consents in BYOD terms. |

## 7.3 Acceptable Use

* Use devices primarily for business; personal use must not interfere with work or violate policy.
* Do not record, photograph, or share customer or confidential information without authorization.
* Disable location sharing for business apps unless required.
* Prohibit installation of unlicensed or high-risk apps; block sideloading on Android.
* Hands-free only when driving where legally permitted; never text or interact with screens while operating a vehicle or machinery.

## 7.4 Data Handling

* Access **restricted** data only via managed apps or virtual desktops; storing restricted data locally is prohibited.
* Classify, retain, and dispose of information per the Information Governance Standard.
* Use company-approved file sync/storage only.

# 8. Information Security Requirements

* **Authentication:** MFA required for all remote access.
* **Least privilege:** Access granted on a need-to-know basis with periodic reviews.
* **Logging/Monitoring:** Remote access and device posture may be monitored for security and compliance; see Privacy Notice.
* **Incident Reporting:** Suspected loss, theft, malware, or data exposure must be reported to Security within **1 hour** at [contact].
* **Third Parties:** Vendors must meet equivalent controls via contract and undergo onboarding review.

# 9. Equipment, Support & Expenses

* **Provided equipment:** [List—e.g., laptop, headset, token].
* **Excluded:** Furniture unless approved as an accommodation; personal peripherals are unsupported.
* **Support:** IT Service Desk [hours/contact] for company-managed devices and apps.
* **Expenses:** Pre-approved, business‑necessary costs (e.g., incremental internet or phone charges) reimbursed per the Expense Policy; receipts required.
* Employees are responsible for home utilities and insurance unless otherwise mandated by law/contract.

# 10. Legal & Compliance

* Remote work does not modify employment at‑will status or exempt employees from local labor, tax, or data protection laws.
* Employees are responsible for ensuring home zoning/lease permits telework; notify insurer/landlord if required.
* Follow records retention, e-discovery, and FOI/subject‑access procedures applicable to your role/jurisdiction.

# 11. Privacy & Monitoring

* To protect [Company] assets, Company may monitor access dates/times, device posture, and corporate app activity on enrolled devices.
* For BYOD, the Company does not access personal photos, personal emails, personal texts, or non-corporate app data; remote wipe targets the corporate container where possible.

# 12. Driving & Safety

* Comply with traffic laws. No manual device interaction or texting while driving.
* If a call is essential, use an approved hands‑device and stop the vehicle when safe to do so.
* Never operate machinery while interacting with a device.

# 13. Insurance & Liability

* Company equipment is covered by corporate insurance when used as intended; employees must take reasonable care.
* Employees are responsible for personal property and any premiums for home insurance unless required otherwise.
* Report incidents (injury, theft, damage) promptly per Health & Safety and Security procedures.

# 14. Compliance & Enforcement

* Violations may result in access revocation, disciplinary action up to termination, vendor off‑boarding, and/or legal action.
* The company may restrict or suspend remote work if risks are not adequately managed.
* **Exceptions** require CISO + HR approval and documented compensating controls.

# 15. Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Summary of change** | **Author** |
| 1.0 | [YYYY-MM-DD] | Initial release | [Name] |

# Appendices (Templates & Checklists)

## Appendix A: Remote Work Agreement (one‑page)

* Employee name/role/manager
* Work location(s) & days
* Work hours & availability
* On-site attendance cadence
* Equipment issued
* Communication tools & cadence
* KPI/Output expectations
* Safety & confidentiality acknowledgments
* Agreement start date, trial period, review date
* Signatures (Employee, Manager, HR)

## Appendix B: Device Enrollment & Minimum Security Checklist

* Device model/OS version within support window
* Full‑disk encryption enabled
* Passcode/biometrics configured (auto‑lock ≤ 5 minutes)
* MDM profile installed; device shows **Compliant**
* Company workspace/app installed; DLP settings active
* VPN auto-connect configured
* Backup to the approved destination only
* Anti-malware enabled (where applicable)
* Lost mode/remote wipe tested

## Appendix C: BYOD Terms (employee attestation)

* Consent to MDM enrollment, posture checks, and selective wipe of corporate data.
* Agreement not to share devices or credentials.
* Acknowledgment of privacy boundaries (no access to personal content).
* Obligation to report loss/theft within 1 hour.
* Termination requirements (remove corporate profiles, return data/equipment).

## Appendix D: Home Workspace Self‑Assessment (condensed)

**Environment & Ergonomics**

* Stable desk/chair; DSE set‑up completed
* Adequate lighting/ventilation
* Tidy area; clear egress; smoke detector present
* Power strips not overloaded; cords secured

**Privacy & Security**

* Screen privacy in place; calls cannot be overheard
* Lockable storage for documents/devices
* Household members/visitors cannot view/access work
* Shredder or secure disposal for confidential paper

**Connectivity**

* Reliable broadband; router firmware current
* VPN available and tested; public Wi‑Fi used only with VPN

**Emergency/Incident**

* Know how to contact IT/Security/HR
* Aware of injury & incident reporting process

## Appendix E: Mobile Device Acceptable Use (quick rules poster)

* Keep OS/apps updated.
* Use strong passcodes; don’t share them.
* Encrypt everything; lock screens quickly.
* Use company apps + VPN only; no personal cloud for work data.
* No texting/typing while driving.
* Report lost/stolen devices immediately.

## Appendix F: Glossary & References

* Link to Information Classification, Access Control, Records Retention, and Acceptable Use policies.