ComplyJet

Remote Work Security Policy Template

A free, adaptable remote work security policy for remote-first and hybrid teams, with sample clauses for locations, the home office, devices and data, hybrid work, lost devices and offboarding, an employee acknowledgement form, a home office attestation and a framework mapping for ISO 27001, SOC 2, HIPAA and NIST.

HOW TO USE THIS TEMPLATE

Replace every [bracketed value] with a real fact about your company. Delete any clause you cannot back with a real control, keep the numbering, and route the final version through your normal approval process, including review by counsel or HR. Locations, windows and review intervals in this template are recommended defaults, not requirements of any standard. Write only what you actually do. Standard references are our summaries, not the text of the standards, so confirm exact wording and scope against the standard itself. This template is not legal advice, and rules on monitoring and cross-border work vary by country.

Company: [Company name]

Policy Owner: [Role, e.g. Head of Operations]

Version: [1.0]

Effective date: [Date]

Approved by: [Name, title]

Next review: [Date, at least annually]

Definitions

Term	Meaning
Remote work	Working with company information away from company premises, including at home, in a co-working space, at a client site, in a public place or while travelling.
Hybrid work	A schedule that splits time between company premises and remote locations.
Approved location	A place listed in the approved locations table, or approved in writing under an exception.
Company-managed device	A device owned or enrolled by the company and covered by its device policies.
Personal device	A device owned by an individual. Allowed for company work only under a documented exception.
Company information	Any customer data, source code, credentials, internal document or other information the company holds, in any form, including paper.

Roles and responsibilities

Role	What they do	Who fills it in a small team
Policy owner	Maintains the policy, the approved locations table and the review schedule	Head of operations or security lead
Policy approver	Approves exceptions, including working from another country	CEO or CTO, never the person requesting
Manager	Approves locations for their team and confirms the baseline at hire	Team lead
HR	Runs onboarding, offboarding and the cross-border check	Head of people, or the founder
IT or security lead	Revokes access, wipes managed devices, keeps the device inventory	Engineering lead or outsourced IT
Employee or contractor	Follows the policy, completes the attestation and reports losses promptly	Everyone in scope

One person may play several roles at a small company. Keep the approver separate from the person asking, so nobody approves their own exception.

Policy clauses

1. Purpose and scope

Clause 1.1 (Purpose and scope (ISO 27001 A.6.7))
[Company] maintains this policy to protect company and customer information when personnel work outside [Company] premises. It applies to all employees, contractors and interns who access, process or store [Company] information away from company premises, whether they work remotely full time or on a hybrid schedule.

2. Eligibility and approval

Clause 2.1 (Eligibility and approval (ISO 27001 A.6.7, SOC 2 CC6.1))
Remote work is available to roles listed in [the remote work register]. Access to [production data and regulated data] may carry additional conditions set by the [Head of Security]. The [Policy Approver] approves exceptions. No person may approve their own exception.

3. Approved locations

Clause 3.1 (Approved locations (ISO 27001 A.6.7, A.7.9))
Personnel may work from home, a co-working space, a client site, a public place or while travelling. In public places, personnel must not hold sensitive calls, must keep the screen out of view of others and must never leave a device unattended. Working from another country requires prior written approval from the [Policy Approver] after review by HR and [legal counsel].

Approved locations (recommended defaults, not a requirement of any standard)

Location	Default rule	Extra conditions	Who approves
Home	Allowed	Home office baseline met and attested	Manager at hire
Co-working space	Allowed	No sensitive calls, privacy screen, device never unattended	Manager
Client site	Allowed	Follow the client's rules where stricter	Manager
Public place	Non-sensitive work	No sensitive calls, no unattended device, screen out of view	Within the policy
Hotel or travel	Allowed	Device kept with you, never in checked luggage or a vehicle	Manager for extended travel
Another country	Approval first	HR and legal review before work starts	Policy approver

4. Home office baseline

Clause 4.1 (Home office baseline (ISO 27001 A.6.7, A.7.7, HIPAA 164.310(b) where applicable))
Personnel must lock their screen when away from the device, must not allow household members or visitors to use or view company devices or information, and must take work calls where they cannot be overheard. Home routers must use a changed default password, current firmware and WPA2 or WPA3. Printing company information at home is not permitted unless the [Policy Approver] has approved it.

5. Devices and data handling

Clause 5.1 (Devices and data handling (ISO 27001 A.7.9, A.8.1, A.5.10, SOC 2 CC6.7, CC6.8))
Company information may be stored and processed only on company-managed devices and approved systems. Personal devices may be used only under an exception granted under the [BYOD Policy]. Company information must not be stored in personal email, personal cloud storage, messaging applications or removable media. Technical device requirements are set out in the [Endpoint Security Policy] and [Mobile Device Management Policy].

6. Hybrid work

Clause 6.1 (Hybrid work (ISO 27001 A.6.7, A.7.7))
Personnel moving between locations must keep devices locked and with them in transit, and must not leave devices or documents in vehicles or checked luggage. When using shared desks or meeting rooms, personnel must clear desks and screens and remove sensitive material from whiteboards before leaving.

7. Lost devices and incident reporting

Clause 7.1 (Lost devices and incident reporting (ISO 27001 A.6.7, SOC 2 CC6.7))
Personnel must report a lost or stolen device, or suspected exposure of company information, to [security channel] within [number] hours of discovery. Prompt reports will not result in disciplinary action for the loss itself. Reports are handled under the [Incident Management Policy].

8. Offboarding and equipment return

Clause 8.1 (Offboarding and equipment return (ISO 27001 A.5.11, A.6.5, SOC 2 CC6.2))
Access rights are revoked on the person's last working day. Personnel must return all company equipment within [number] days using the courier arrangement provided. [Company] may remotely wipe managed devices. Personnel who used a personal device by exception must confirm in writing that company information has been deleted.

9. Monitoring boundary

Clause 9.1 (Monitoring boundary (ISO 27001 A.6.7))
[Company] monitors company-managed devices and company systems only to the extent described in [the Acceptable Use Policy] and permitted by applicable law. [Company] does not collect personal browsing, home network traffic or personal files. [Counsel to review this clause for each country of operation.]

10. Acknowledgement, enforcement and review

Clause 10.1 (Acknowledgement, enforcement and review (ISO 27001 A.6.7, A.6.3, SOC 2 CC6.1))
All personnel acknowledge this policy in writing on joining and at least [annually]. Breaches may lead to disciplinary action in line with [Company] policy. The [Policy Owner] reviews this policy at least [annually] and after any material change to how or where personnel work.

Framework mapping

Policy section	ISO 27001 hook	SOC 2 evidence commonly tested	HIPAA (if applicable)	NIST
Eligibility and approval	A.6.7	Policy, approvals, access records (CC6.1, CC6.2)	164.310(b)	SP 800-46
Approved locations	A.6.7, A.7.9	Policy, location approvals	164.310(b)	SP 800-46
Home office baseline	A.6.7, A.7.7	Acknowledgements and attestations	164.310(b), (c)	SP 800-114 for the user
Devices and data handling	A.7.9, A.8.1, A.5.10	Device inventory (CC6.7, CC6.8)	164.310(c)	SP 800-46
Lost devices and offboarding	A.5.11, A.6.5	Offboarding records (CC6.2)	164.310(d)(1)	SP 800-46

The SOC 2 column describes how auditors commonly test remote work; SOC 2 has no named remote work criterion. HIPAA applies only to covered entities and business associates. ISO control titles are our short summaries, so check the exact wording in ISO/IEC 27001:2022 and 27002:2022.

Appendix A: employee acknowledgement form

Acknowledgement

I have read and understood the Remote Work Security Policy of [Company]. I will work only from approved locations, keep company information on company-managed devices unless an exception has been granted, follow the home office baseline, report a lost or stolen device or suspected exposure within [number] hours, and return all company equipment within [number] days when my work ends.

Name: [ ] _____

Signature: [ ] _____

Date: [ ] _____

Appendix B: home office baseline attestation

Complete at hire and at each [quarterly] attestation. Tick each item that is true today.

Done	Baseline item
[ ]	I lock my screen whenever I step away from the device
[ ]	Nobody else in my household uses my work device or sees company information
[ ]	I take work calls where they cannot be overheard
[ ]	My home router has a changed default password, current firmware and WPA2 or WPA3
[ ]	Visitors and smart home devices use a guest network
[ ]	I keep company data out of personal email, personal cloud storage and removable media
[ ]	I do not print company information at home unless it has been approved

Name: [ ] _____ **Signature:** [ ] _____ **Date:** [ ] _____

Appendix C: customization checklist

Before you edit a single clause, gather these facts:

- Headcount and the countries people work from
- Whether you are remote-first or hybrid, and whether you use a co-working space
- Which devices are company-managed and which, if any, are personal
- Whether any regulated data is in scope, such as ePHI
- Who approves exceptions and who owns the policy
- The reporting window, the equipment return window and the review cycle

Evidence checklist

- Approved policy with version and date
- Signed acknowledgements
- Location approvals and overseas exceptions
- Device inventory
- Training records
- Home baseline attestations
- Offboarding and equipment-return records

Revision log

Version	Date	What changed	Approved by
[1.0]	[Date]	[Initial version]	[Name]
[ ]	[ ]	[ ]	[ ]

This template is general information, not legal advice. Have counsel or HR review the final policy. Free to use and adapt. Published by ComplyJet: complyjet.com/blog/remote-work-security-policy