Logo da Empresa

Remote Work Policy

Version: 1.0

Classification: Internal

Document Owner: XX Information Security Team

Last Reviewed: 01/06/2025

Revision History

Version	Revision Date	Reviewer
1.0	2025/06/01	init

Content

Remote Work Policy

Purpose

The purpose of this policy is to establish clear requirements for employees and authorised third parties who perform mobile or remote work. The aim is to ensure the confidentiality, integrity, and availability of company information and systems when accessed or processed outside of secure corporate environments.

Scope

This policy applies to all employees and authorised third-party users who access, process, or store company information while working remotely or using mobile devices. It covers both company-owned and personally-owned devices (Bring Your Own Device – BYOD) used for company purposes.

Mobile Working Guidelines

Device Security

All devices used for company work must:

- Be secured with strong authentication (passwords, PINs, biometrics)
- Have full-disk encryption enabled
- Include and regularly update anti-malware protection
- Be set to auto-lock after a defined period of inactivity
- Be registered with the company for inventory and remote management

Physical Protection of Devices

When connecting through public or untrusted networks, users must:

- Use a company-approved VPN at all times

- Avoid accessing or transmitting sensitive data unless VPN encryption is active
- Disable automatic Wi-Fi connection to known public hotspots

Handling of Confidential Information

When working in mobile settings:

- Apply Clear Desk and Clear Screen principles
- Avoid exposing confidential data on screens or printed material in public spaces
- Secure paper records in transit (e.g., locked bags)
- Use shredders or confidential disposal bins as per the Information Destruction Policy.

Incident Reporting

Any suspected or actual loss, theft, or compromise of a device or information must be reported immediately to the Information Security team, following the Incident Management Procedure.

Remote Working Guidelines

Secure Workspace Setup

Remote workers must maintain a secure, dedicated workspace that limits access to authorised personnel only. Screens should not be visible to family members, guests, or the public.

Network and Connectivity Security

All remote access must:

- Use a company-approved VPN connection
- Be performed over secured home networks protected by strong Wi-Fi passwords and up-to-date router firmware

- Prohibit the use of open, unprotected Wi-Fi for company work unless VPN is active

Device Provisioning and BYOD

Whenever possible, employees should use company-issued devices. If BYOD is authorised, the following conditions apply:

- The device must meet the company's minimum security standards
- Security configurations (e.g., VPN, encryption, antivirus) must be enforced
- Ensure the licensing of software used in the work context
- Ensure access to network shares through authentication and segregation of privileges

Data Access and Storage Practices

Users must:

- Access data via authorised cloud platforms or company servers (e.g., through VPN or web portals)
- Never store company data on unapproved personal devices or local folders
- Not sync company information to personal cloud accounts (e.g., Dropbox, iCloud) without prior approval
- A form is used to clearly indicate the required access and an authorisation email or signature is provided.

Use of Communication Tools

Only company-approved communication platforms may be used to discuss or share confidential information. This includes video conferencing, email, chat, and file sharing.

Legal and Regulatory Compliance

Remote work must be compliant with local laws, particularly regarding data protection, employment, and cybersecurity. Users must inform the company of any jurisdictional constraints affecting their remote working arrangement.

Security Awareness and Training

All mobile and remote workers must:

- Complete mandatory training on remote working security prior to engaging in remote work
- Undergo periodic refresher training covering:
    - Phishing and social engineering risks
    - Proper handling of personal and confidential data
    - Incident reporting and physical security
    - Secure use of communication tools

Related Documents

Acceptable Use of Assets Policy

Information Security Policy

Clear Desk and Clear Screen Policy

Information Classification & Handling Policy

Policy Compliance

Compliance Measurement

The Security Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager.

Non-Compliance

Any employee found to be in breach of this policy may be subject to disciplinary proceedings, in accordance with the applicable provisions of the Portuguese Labour Code. Where justified, this may include the formal initiation of a disciplinary process, with the issuance of a statement of offence (“nota de culpa”), and may lead to sanctions up to and including dismissal.

Continual Improvement

This policy is reviewed and updated whenever necessary and at least once per year.