Remote Working Policy

*[Company Name] | Effective date: [YYYY-MM-DD] | Version: 1.0*

# 1. Purpose

This Remote Working Policy (“Policy”) defines the standards and expectations for employees who work from home or from locations other than Company premises.

It supports flexible work while protecting productivity, security, confidentiality, and wellbeing.

# 2. Scope

Applies to all employees, contractors, and interns approved for full-time, part-time, or occasional remote work.

This Policy works alongside the Code of Conduct, IT Security Policy, and Data Privacy Policy. In case of conflict, the stricter requirement applies.

# 3. Eligibility & Approval

Eligibility depends on role requirements, performance, and team needs.

Employees must obtain manager approval and, where required, HR approval before commencing remote work.

A Remote Work Agreement must be completed, stating schedule, location(s), equipment, and any conditions.

# 4. Remote Work Locations

Primary remote location should be a private residence or other approved site within the employee’s country of employment unless otherwise authorized.

Working from another country requires prior written approval due to tax, labor law, data protection, and export control implications.

# 5. Working Hours, Availability & Attendance

Employees are expected to maintain their standard working hours unless otherwise agreed.

Be available on core collaboration hours: [e.g., 10:00–15:00] in the employee’s local time zone.

Record time using approved systems; notify your manager of unavailability (e.g., illness, emergencies).

Attend mandatory meetings (virtual or on-site) when requested with reasonable notice.

# 6. Communication & Collaboration

Use approved channels (e.g., email, chat, video conferencing) for business communication.

Keep calendars up to date and set status/availability indicators appropriately.

Turn on video when requested for key meetings if bandwidth permits and a suitable environment is available.

# 7. Workspace Standards & Ergonomics

Choose a safe, quiet, and professional workspace with reliable internet connectivity.

Follow ergonomic best practices and report discomfort early; the Company may provide guidance or resources.

Keep work areas free from unauthorized individuals' access to Company information.

# 8. Equipment & Expenses

Company may provide necessary equipment (e.g., laptop, monitor, peripherals) for business use.

Employees must care for Company assets, report damage/theft promptly, and return items upon request or termination.

Expenses (e.g., data, phone, office supplies) must comply with the Expense Policy and receive pre-approval where required.

# 9. Information Security & Privacy

Comply with the IT Security Policy and Data Privacy Policy at all times.

Use Company-managed devices with disk encryption, EDR/antivirus, and up-to-date patches.

Use MFA and approved VPN/ZTNA for remote access; do not share accounts or passwords.

Avoid public Wi‑Fi where possible; if used, connect via VPN and do not access Restricted data in public spaces.

Lock screens when away; store documents securely; shred or securely dispose of confidential materials.

# 10. BYOD (Bring Your Own Device)

Personal devices used for work must meet security requirements and, where applicable, be enrolled in MDM/MAM.

Restricted data may not be stored on personal devices unless explicitly approved with compensating controls.

The Company may require removal of Company data or apps from personal devices upon role change or termination.

# 11. Data Protection & Confidentiality

Handle Personal Information in line with POPIA and, where applicable, GDPR/UK GDPR.

Discuss confidential matters in private settings only; use headsets to prevent eavesdropping.

# 12. Health, Safety & Incident Reporting

Employees are responsible for maintaining a safe remote work environment and complying with health and safety guidance.

Report injuries, hazards, and work-related incidents promptly via the normal reporting channels.

Report suspected data/security incidents immediately to Security at [security@company.com] and the DPO/IO at [privacy@company.com].

# 13. Performance Management

Performance standards and objectives remain the same regardless of work location.

Managers will review productivity, quality, and communication regularly and may adjust arrangements where necessary.

# 14. Travel & On-Site Requirements

Employees may be required to attend on-site meetings, training, or customer visits with reasonable notice.

Travel expenses are subject to the Expense Policy and pre-approval requirements.

# 15. Monitoring & Acceptable Use

Use of Company systems may be monitored in accordance with applicable laws and the Acceptable Use Policy.

Do not use Company systems or data for personal gain, illegal activity, or to create a hostile environment.

# 16. Security & Compliance Checks

The Company may conduct remote audits of compliance with this Policy (e.g., endpoint posture checks, configuration verification).

Periodic attestations of policy compliance may be required.

# 17. Cross-Border & Tax Considerations

Remote work from outside the country of employment may create legal, payroll, tax, and immigration implications.

Employees must obtain written approval before working outside their approved jurisdiction.

# 18. Revocation of Remote Work

The Company may modify or revoke remote work arrangements due to performance concerns, business needs, role changes, or policy violations.

Employees will receive reasonable notice where possible.

# 19. Related Policies & Documents

Code of Conduct • IT Security Policy • Data Privacy Policy • Acceptable Use Policy • Expense Policy • Health & Safety Guidance • Incident Response Plan.

# 20. Employee Acknowledgment

I acknowledge that I have read and understand this Remote Working Policy and agree to comply with it.

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_

# 21. Review & Change History

This Policy will be reviewed at least annually or when material changes occur.

Version 1.0 — Initial release on [YYYY-MM-DD].

*This document is uncontrolled if printed. Verify the latest version on the Company policy portal.*