INSERT LOGO

REMOTE WORKING POLICY

Classification: Internal

This document may only be shared internally without prior confirmation from the owner.

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Contents

1. Purpose

This document outlines the policies and procedures for remote working to ensure the security and integrity of [Company Name]'s information assets, maintain productivity, and ensure compliance with relevant laws and regulations.

2. Scope

This Remote Working Policy applies to:

- All employees, contractors, and third-party users accessing [Company Name] information systems and data from remote locations.

3. Responsibilities

Line Managers:

- Ensure team members are aware of and comply with remote working policies.
- Monitor remote workers' performance and security compliance.

Employees:

- Follow the remote working procedures and security guidelines outlined in this policy.
- Report security incidents or breaches immediately.

IT Department:

- Provide and maintain secure remote access solutions.
- Monitor remote access and enforce security protocols.
- Provide support and training for secure remote working.

4. Exceptions

- Seek exceptions through the IT Helpdesk, with approval required from IT and management.

5. Remote Access Control

- **VPN Usage:** Employees must use the company-approved VPN for all remote connections to [Company Name] networks.
- **Multi-Factor Authentication (MFA):** Enable MFA to access sensitive systems and data.
- **Encryption:** Ensure all remote connections are encrypted.

6. Device Security

- **Software Updates:** Keep all devices updated with the latest security patches and antivirus software.
- **Passwords:** Use strong passwords or passphrases and change them regularly.
- **Device Encryption:** Enable full-disk encryption on all devices used for remote work.

7. Data Handling and Storage

- **Cloud Storage:** Use company-approved cloud storage solutions to save and share documents.
- **Local Storage:** Avoid storing sensitive company data on local drives or personal devices.

- **Data Transfer:** Ensure all data transfers are conducted over secure, encrypted channels.

8. Incident Reporting

- **Identify Incidents:** Recognize signs of potential security incidents, such as phishing emails or unusual system behaviour.
- **Report Incidents:** Immediately report any suspected security incident to the IT helpdesk.
- **Incident Response:** Follow the company's incident response plan for remote working scenarios.

9. Physical Security

- **Secure Workspace:** Set up a remote workspace in a private area and use privacy screens if working in shared or public spaces.
- **Device Protection:** Lock screens when devices are unattended and use strong passwords or biometrics to unlock devices.

11. Monitoring and Compliance

- **Regular Audits:** IT will audit remote access logs and device compliance monthly.
- **Employee Compliance:** Employees must complete security training and report non-compliance or policy violations.

12. References

- Acceptable Use Policy
- BYOD Policy
- Information Security Policy
- Incident Response Plan
- [Any other relevant documents]