1. Remote Work Policy 1.1 Eligibility

- Remote work is allowed for roles approved by the employee's manager and IT Operations.
- Employees must maintain a stable internet connection and a private work environment.

1.2 Working Hours and Availability

- Employees must be available during core hours: 10:00–16:00 local time.
- Meetings should be scheduled with at least 24 hours' notice unless urgent.

1.3 Workspace Requirements

- A separate, well-lit workspace free of excessive noise is required.
- Sensitive conversations should not take place near smart assistants or shared devices.

2. IT Equipment Policy 2.1 Standard Equipment

- Employees receive a standard laptop, charger, and basic peripherals.
- Additional peripherals (e.g., external monitors) require manager approval.

2.2 Exceptions

- Exceptions to standard equipment must be requested via the IT Equipment Request Form and approved by the employee's manager and IT Operations.

2.3 Equipment Return

- Upon role change or termination, equipment must be returned within 5 business days.

3. Device Security 3.1 Mandatory Controls

- Full-disk encryption must be enabled on all company-issued laptops.
- Screen lock set to 5 minutes of inactivity.
- OS and security patches must be installed within 3 business days of release.

3.2 Antivirus and EDR

- Approved antivirus and endpoint detection/response (EDR) tools must be active at all times.
- Tampering with security software is prohibited.

3.3 Removable Media

- Only IT-approved encrypted USB devices may be used.
- Personal USB storage is not permitted for company data.

4. Network Access 4.1 VPN Usage

- VPN is required to access internal systems from outside corporate offices.
- Multi-Factor Authentication (MFA) must be used for all VPN logins.

4.2 Public Wi-Fi

- Public Wi-Fi may be used only with VPN enabled.
- Avoid performing privileged administrative actions on public networks.

5. Data Handling 5.1 Classification

- Company data must be handled per its classification (Public, Internal, Confidential).
- Confidential data may not be stored on personal devices.

5.2 Cloud Storage

- Use only IT-approved cloud storage with company SSO.
- Sharing links must expire in 14 days unless extended by a manager.

6. Incident Reporting 6.1 What to Report

- Lost/stolen device, suspected malware, phishing, unauthorized access, or data exposure.

6.2 Reporting Timeline

- Security incidents must be reported within 24 hours of discovery.

6.3 How to Report

- Submit an Incident Report via the IT Service Portal and notify your manager.
- For urgent issues, contact the IT Security hotline listed in the portal.

7. Travel & Temporary Access 7.1 Travel Notice

- Notify IT at least 3 business days before international travel to ensure regional access and device compliance.

7.2 Temporary Admin Access

- Request via IT Service Portal with justification and time-bound duration.
- Approvals expire automatically and must be re-requested if needed.