IT & Data Security Policy

1. Device Usage

Company-issued laptops and devices must be used primarily for business purposes. Full-disk encryption must be enabled on all devices.

Employees must lock their screens when stepping away from their workstation (Win+L or Cmd+Ctrl+Q).

Personal devices may be used for work only if enrolled in the company's Mobile Device Management (MDM) solution.

2. Password & Access Policy

All system passwords must be at least 12 characters long and include uppercase, lowercase, numbers, and special characters.

Passwords must be changed every 90 days. Password reuse (last 6 passwords) is prohibited.

Multi-factor authentication (MFA) is mandatory for all company email accounts, VPN, and cloud services.

Employees must not share passwords or access credentials under any circumstances.

3. Data Classification

Company data is classified into four levels: Public, Internal, Confidential, and Restricted.

Confidential and Restricted data must not be stored on personal devices, personal cloud storage (Google Drive personal, Dropbox personal), or shared via personal email.

All Restricted data must be encrypted at rest and in transit.

4. Acceptable Internet Use

Internet access is provided for business use. Streaming video, online gaming, and accessing adult content on company networks or devices is prohibited.

Employees must not download software from untrusted sources or disable company-installed security tools (antivirus, EDR).

5. Incident Reporting

Any suspected security incident — phishing email, malware, data loss, unauthorised access — must be reported to security@company.com or IT helpdesk within 2 hours of discovery.

Do not attempt to investigate or remediate security incidents independently. Isolate the affected device and contact IT immediately.

6. Remote Access & VPN

Employees must use the company VPN when accessing internal systems or confidential data from outside the office.

Use of public Wi-Fi without VPN for company work is strictly prohibited.