Access Control Policy

1. Purpose

The purpose of this Access Control Policy is to ensure the security and confidentiality of sensitive business and healthcare information. This policy outlines guidelines and procedures for granting, managing, and revoking access to company resources and patient data to maintain regulatory compliance and protect against unauthorised access.

2. Scope

This policy applies to all employees, contractors, and third-party vendors accessing company systems, applications, and patient data remotely.

3. Access Control Measures

3.1 User Authentication

- All employees must use strong, unique passwords for their accounts.
- Multi-factor authentication (MFA) is mandatory for accessing company systems and applications.
- MFA methods may include SMS, email, authenticator apps, or hardware tokens.

3.2 Account Provisioning and De-provisioning

- User accounts will be created, modified, or deactivated by authorised personnel only.
- Accounts will be provisioned based on the principle of least privilege, granting access only to the resources necessary for the employee's role.
- Accounts will be deactivated or removed promptly upon employee termination or role change.

3.3 Remote Access Tools

- Authorised remote access tools and VPNs will be provided for secure connections to company resources.
- Remote desktop access will be allowed only through encrypted and secure channels.

3.4 Data Encryption

- All remote access connections will be encrypted using strong encryption protocols (e.g., TLS) to protect data in transit.

4. Employee Access

Access to company systems and patient data will be controlled based on roles and responsibilities.

4.1 Employee Roles and Access

- Employee roles will be defined based on job responsibilities and need-to-know basis.
- Employees will have access only to the resources necessary for their job functions.

5. Data Access and Handling

5.1 Patient Data Access

- Access to patient health records and sensitive medical information will be restricted to authorised personnel only.

5.2 Remote Data Storage and Transfer

- Employees working online using their own computer must store sensitive data only on Google Drive, never on their hard drive.
- Patient data should be transferred using their online patient profile in the booking and patient management software.

6. Incident Response

6.1 Reporting Incidents

- Employees are required to report any suspected security incidents or unauthorised access immediately to their manager.

6.2 Incident Management

- The company will have an incident response plan in place to address security breaches and unauthorised access promptly.
- Affected employees will be informed as per legal requirements and company policies.

8 Policy Acknowledgment

- All employees must acknowledge and agree to abide by this Access Control Policy before being granted access to company resources and software.