REMOTE ACCESS POLICY

Remote Access and BYOD Policy

1. Purpose The purpose of this policy is to establish guidelines for remote access to the Institute's internal network via a Virtual Private Network (VPN) and to regulate the use of personal devices (BYOD) to access institutional resources. This policy aims to enhance security, ensure compliance and minimise the risks associated with remote access and the use of personal devices.

2. Scope This policy applies to all employees, contractors, suppliers and other third parties who require remote access to the organisation's internal network. It also applies to all personal devices (BYOD) used to access the organisation's network, systems and data.

3. Guidelines for remote access

3.1. VPN access requirements

- VPN access must be requested and approved by the IT department.
- Users are issued with a username and password, which are used for authentication prior to accessing the network.
- Access will be granted on a least-privilege basis.
- VPN connections should only be initiated from secure devices that meet security compliance requirements.

3.2. Restrictions on use

- Remote access must be used exclusively for the official purposes of the Institute.
- Users must not share their VPN credentials with unauthorised persons.
- The use of public or unsecure networks to access the VPN is prohibited.
- Users must log out of VPN sessions when they are no longer in use.

3.3. Monitoring and compliance

- All VPN connections will be logged and monitored for suspicious activity.
- The organisation reserves the right to review remote access logs and enforce compliance with the policy.
- Any unauthorised access detected will result in the immediate disconnection and deactivation of the account.

4. Guidelines for BYOD (Bring Your Own Device)

4.1. Device Registration and Security Requirements

- Employees must register their personal devices with the IT department before gaining access to company resources.
- Devices must have up-to-date security patches and operating system updates.
- Antivirus and endpoint protection software must be installed and updated regularly.
- Devices must be encrypted and require a secure password, biometric authentication or an equivalent security mechanism.

4.2. Acceptable use

- Personal devices may only be used for specific Institute purposes when connected to the corporate network.
- Users are prohibited from downloading, storing or transmitting sensitive company data on personal devices, unless they have received specific authorisation to do so.
- The use of jailbroken or rooted devices for corporate access is strictly prohibited.

4.3. Data protection and loss prevention

- Users must immediately report the loss or theft of personal devices to the IT department.
- Users must not back up company data to unauthorised cloud storage or personal accounts.

4.4. Compliance and Monitoring

- The IT Department reserves the right to monitor compliance with the BYOD policy and to enforce security measures.
- Non-compliant devices will be denied access to the corporate network.
- Users who do not comply with the BYOD security requirements may face disciplinary action, including the revocation of access privileges.

5. Responsibilities

5.1. Employee responsibilities

- Ensure that personal devices meet all security and compliance requirements.

- Remote access and personal devices must be used responsibly and in accordance with the Institute's policies.
- Report any security breaches or suspicious activity to the IT department immediately.

5.2. Responsibilities of the IT department

- Maintaining and enforcing VPN security policies.
- Providing guidance and support to employees who use personal devices for work.
- Monitoring and investigating remote access activities to identify security threats.
- Ensuring regular updates and improvements to VPN and BYOD security measures.

6. Policy violations and consequences

- Breach of this policy may result in disciplinary action, including the revocation of access privileges, suspension or dismissal.
- In cases of data breaches, unauthorised access or misuse of the Institute's resources, legal action may be taken.

7. Review and updating of the policy

- This policy will be reviewed annually by the IT and security teams to ensure compliance with evolving security standards.
- Updates to the policy will be communicated to all employees, and confirmation of understanding and compliance will be required.

By accessing the organisation's network remotely or using a personal device for work purposes, users acknowledge and agree to comply with this policy.