VPN Usage Guidelines for Offsite Access

Purpose

These guidelines define the proper and secure use of VPN connections by employees who require offsite access to organizational resources. All staff must adhere to these practices to maintain data security and privacy.

Scope

This guideline applies to all employees, contractors, and external partners who connect to the organizationâ€™s network remotely via VPN.

Guidelines

1. Use VPN strictly for work-related purposes and access only authorized resources.
2. Always authenticate using your assigned credentials. Never share your login information.
3. Keep your deviceâ€™s operating system and antivirus software up to date before connecting to VPN.
4. Log out from VPN when remote work is finished or when the device is left unattended.
5. Do not download, transmit or store sensitive data outside authorized organizational applications.
6. Report any suspicious activity or security incidents to IT immediately.
7. Do not attempt to bypass or disable VPN security measures.
8. Access to VPN may be monitored or reviewed for compliance and security.

Responsibilities

- **Users:** Follow these guidelines at all times while using VPN for offsite access.
- **IT Department:** Provide support, maintain VPN infrastructure, and monitor network activities.

Compliance

Any violation of these guidelines may lead to disciplinary action and/or revocation of VPN access privileges.