VPN Usage Guidelines

When to Use VPN

Always use company VPN when accessing company resources from outside the office network. This includes email, file shares, internal applications, and databases.

VPN is required when working from home, coffee shops, hotels, or any non-company network. Public WiFi networks are particularly risky without VPN.

VPN Client Installation

Download the approved VPN client from the IT portal. Installation guides are available for Windows, Mac, Linux, iOS, and Android.

Contact IT helpdesk if you encounter installation issues. VPN client must be kept updated to latest version for security patches.

Connecting to VPN

Launch VPN client and enter your company credentials. Enable multi-factor authentication when prompted. Select appropriate VPN gateway for your region.

Connection typically establishes within 30 seconds. Green indicator shows successful connection. All traffic is now encrypted and routed through company network.

Split Tunnel vs Full Tunnel

Our VPN uses split tunneling - only company traffic goes through VPN, personal traffic uses your regular internet connection.

This improves performance for personal browsing while securing company data. Don't attempt to modify tunnel configuration.

VPN Performance

VPN may slightly reduce internet speed due to encryption overhead. If experiencing significant slowness, try different VPN gateway or check your internet connection.

Disconnect and reconnect if VPN becomes unresponsive. Contact IT if problems persist.

Troubleshooting Common Issues

Cannot connect: Verify internet connection, check credentials, ensure MFA device is available. Try different network if on public WiFi.

Frequent disconnections: Check for VPN client updates, verify network stability, contact IT if issue continues.

Slow performance: Try different VPN gateway, close unnecessary applications, check local network speed.

Security Considerations

Never disable VPN to access company resources faster. Don't share VPN credentials. Report suspicious VPN activity to security team.

VPN logs are monitored for security purposes. Unusual patterns may trigger security review.

Mobile VPN Usage

Install VPN profile on mobile devices accessing company email or data. VPN should auto-connect when accessing company resources.

Keep VPN app updated. Battery usage may increase when VPN is active. Disconnect when not accessing company resources to save battery.

VPN for Travel

When traveling internationally, connect to VPN before accessing company resources. Some countries restrict VPN usage - check local laws.

VPN may be slower due to distance from gateways. Plan accordingly for time-sensitive work.