Set Up and Enforce VPN for Remote Work

This checklist ensures that remote work is conducted securely, sensitive data remains protected, and unauthorized access is minimized.

 # 1. Plan the VPN Deployment

☐ Identify the resources and systems that need to be accessed securely via the VPN.
☐ Choose a VPN solution suitable for your organization (e.g., OpenVPN, WireGuard).
☐ Allocate sufficient hardware and bandwidth for the VPN server.

#2. Set Up the VPN Server

☐ Install and configure the VPN server software (OpenVPN, WireGuard, etc.) on a secure server.
☐ Generate and distribute necessary VPN keys, certificates, or credentials for authentication.
☐ Configure the server to enforce strong encryption protocols (e.g., AES-256 for OpenVPN).
☐ Set up routing rules to allow secure access to internal resources while blocking unnecessary traffic.

#3. Configure Client Devices

☐ Install VPN client software on all user devices (desktops, laptops, and mobile devices).
☐ Provide users with configuration files or credentials to connect to the VPN.
☐ Test the connection on various devices to ensure compatibility and stability.

#4. Enforce VPN Usage

☐ Configure company policies to require all remote work activities to go through the VPN.
☐ Set up firewall rules to block remote access to internal resources from non-VPN IP addresses.
☐ Require employees to use the VPN when accessing sensitive data or company resources.

#5. Enhance Security

☐ Enable multi-factor authentication (MFA) for VPN access.
☐ Restrict VPN access to specific employees or devices as needed.
☐ Regularly update VPN server and client software to patch vulnerabilities.

#6. Monitor and Maintain the VPN

☐ Use logging and monitoring tools to track VPN usage and identify unauthorized access attempts.
☐ Conduct regular audits of VPN user accounts and permissions.
☐ Collect user feedback to improve connection performance and reliability.

#7. Educate Employees

☐ Train employees on how to connect to and use the VPN securely.
☐ Provide guidelines for secure remote work practices, including VPN usage requirements.

Need a hand with the next step?

If you have a question about any of these steps, or need help setting up a more advanced or tailored solution, we're here for you!

Feel free to send us an email at contact@403bits.com.

For simpler queries, we'll gladly share advice or point you in the right direction — free of charge!

And if you're facing a more complex challenge or want to save time, our experts can take over and deliver a comprehensive setup that perfectly fits your needs.

We're here to help you build security and efficiency
so you can focus on growing your business!

If you liked this checklist or have improvement suggestions, - let us know contact@403bits.com.