IT VPN & NETWORK CONNECTIVITY GUIDE

Department: IT Support
Category: VPN & Network
Audience: All Employees
Purpose: Provide instructions, troubleshooting steps, and best practices for VPN and network access.

---

1. Overview

The company requires all employees working remotely or accessing internal systems offsite to use a **Virtual Private Network (VPN)**.
VPN ensures **secure access** to internal resources and protects sensitive company data.

Network connectivity is essential for email, cloud tools, and collaboration platforms.

---

2. Supported VPN Clients

- **OpenVPN** (Windows / Mac / Linux)
- **Cisco AnyConnect** (Windows / Mac / Linux)
- **FortiClient** (Optional for secure access)

All clients must be installed and configured according to IT guidelines.

---

3. VPN Access Eligibility

- Full-time employees with company credentials
- Valid network login ID
- Active HR and IT approval

---

4. VPN Installation & Configuration

4.1 OpenVPN

1. Download installer from company VPN portal
2. Install the application
3. Import configuration file provided by IT
4. Login using company credentials

4.2 Cisco AnyConnect

1. Download client from IT portal
2. Install & accept default options
3. Connect using VPN server address
4. Enter company username/password

4.3 Common Settings

- Enable **auto-reconnect**
- Always verify **certificate validity**
- Update VPN client monthly

---

5. Common VPN & Network Issues

5.1 VPN Not Connecting

Possible Causes:

- Incorrect username or password
- Expired credentials
- Firewall or antivirus blocking VPN
- Network restrictions

Troubleshooting Steps:

1. Verify credentials
2. Restart VPN client and computer
3. Check firewall/antivirus settings
4. Try alternate network
5. Contact IT if issue persists

5.2 Authentication Failed

- Incorrect login details
- Two-factor authentication not completed

Action: Reset password via IT portal and retry login.

5.3 Slow VPN / Network Speed

- Network congestion
- High VPN server load
- Background apps consuming bandwidth

Action:

1. Close unnecessary apps
2. Switch to wired connection if possible
3. Retry during off-peak hours

5.4 Network Access Restrictions

- Some internal apps are restricted by department or role
- Access may require IT approval

Action: Submit IT access request ticket for additional permissions.

---

6. Security Guidelines

- Never share VPN credentials
- Always disconnect when not in use
- Use company-provided devices for VPN
- Report suspicious network activity immediately

---

7. When to Raise a Ticket

Raise a ticket for:

- VPN client not installing or connecting
- Authentication issues
- Continuous network slowdown
- Access denied to internal apps
- Any unresolved VPN issue after 30 minutes of troubleshooting

---

8. Information Required While Raising VPN / Network Ticket

- Employee ID
- Device type (Windows / Mac / Linux)

- VPN client version
- Error message / screenshot
- Steps already attempted