

Remote & VPN Access Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Version: 1.2

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

Document Revision History:

VERSION NO.	REVISION DATE	AUTHOR	REVIEWED BY	APPROVED BY	DESCRIPTION
1	28/6/2022	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed
1.1	28/6/2023	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed
1.2	28/7/2024	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed

1. Purpose

The purpose of this **Remote Access Policy** is to define the principles, guidelines, and procedures for providing secure remote access to the company's network and systems. This policy ensures that remote access is granted in a controlled, secure, and compliant manner while minimizing risks to the company's sensitive data and systems.

2. Scope

This policy applies to:

- All employees of [Your Company Name], including full-time, part-time, contractors, and temporary workers.
- Third-party vendors or partners who require access to [Your Company Name] systems.
- Remote access to internal company resources, including networks, databases, applications, and sensitive data.

3. Remote Access Methods

Remote access to company systems will be provided through the following methods:

- **Virtual Private Network (VPN):** The primary method for accessing the company network remotely.
- **Remote Desktop Protocol (RDP):** For specific use cases, access to company desktops or servers.
- **Cloud-Based Applications:** Web-based access to company applications hosted on cloud platforms.

4. Remote Access Requirements

To maintain a secure remote access environment, the following requirements must be met:

- **Multi-Factor Authentication (MFA):** MFA must be used to authenticate users before granting remote access.
- **Device Security:** Remote devices must have up-to-date antivirus software, firewalls, and encryption enabled.
- **Strong Password Policy:** Remote access passwords must comply with the company's strong password policy.
- **Access Logs and Monitoring:** All remote access activity must be logged and regularly monitored to detect unauthorized access.
- **VPN Connection:** All employees must use the company's approved VPN service to access internal systems. Direct connections to internal resources without VPN are prohibited.
- **Encryption:** All data transmitted over remote access connections must be encrypted to protect sensitive information.
- **User Access Control:** Access will be granted based on the principle of least privilege. Users will only be granted access to the specific systems and resources necessary for their role.

5. User Responsibilities

Users of remote access must adhere to the following responsibilities:

- **Secure Devices:** Users must ensure that their remote devices are secure, including using device encryption and setting strong passwords.
- **Compliance:** Users must comply with all company policies and procedures related to data security, confidentiality, and usage while accessing company resources remotely.
- **Reporting Security Incidents:** Any security incidents, such as lost or stolen devices or suspected unauthorized access, must be reported immediately to the IT department.
- **Session Timeouts:** Remote sessions must be configured to time out automatically after a period of inactivity (e.g., 15 minutes).

6. Access Approval Process

- **Requesting Access:** Employees, contractors, or third parties requesting remote access must submit a formal request via the company's access request system.

- **Approval Process:** Requests will be reviewed by the IT Security Team to ensure the need for remote access is legitimate and that the requester meets all necessary security requirements.
- **Access Granting:** Upon approval, remote access credentials (including VPN credentials and MFA setup) will be provided, and the user will be given access to required resources.
- **Revocation of Access:** Remote access will be revoked upon the termination of employment or contract, or when access is no longer required.

7. Security Controls

- **Firewall Rules:** Remote access is allowed only through the company's VPN and is subject to firewall rules designed to limit access to only approved systems.
- **Endpoint Security:** All remote devices must have company-approved endpoint security measures (e.g., antivirus software, disk encryption, etc.) to reduce the risk of malware or data theft.
- **Periodic Reviews:** Remote access privileges will be reviewed periodically (e.g., quarterly) to ensure compliance and eliminate unnecessary access.

8. Monitoring and Enforcement

- **Audit Trails:** All remote access activity will be logged, including login times, IP addresses, and accessed systems. Logs will be monitored by the IT Security Team for unusual or unauthorized activity.
- **Enforcement:** Violations of this policy may result in the revocation of remote access privileges and disciplinary action in accordance with company guidelines.

9. Training and Awareness

- **Security Awareness:** All users granted remote access must undergo security training that covers the safe use of remote access technologies, common threats, and how to avoid them.
- **Periodic Refresher Training:** Users will receive periodic refresher training to ensure they stay informed of new security threats and best practices.

10. Conclusion

The **Remote Access Policy and Procedures** aim to ensure secure access to BPO Convergence Pvt Ltd's resources while safeguarding the confidentiality, integrity, and availability of sensitive company data. Adherence to these procedures will mitigate risks related to remote working and ensure compliance with security standards.