SOP Template: Remote Support and Access Procedures

1. Purpose

This Standard Operating Procedure (SOP) defines **remote support and access procedures**, including secure authentication methods, authorized user access protocols, remote session initiation guidelines, data protection measures, troubleshooting and technical support processes, and logging and monitoring activities. The objective is to ensure secure, efficient, and controlled remote access to systems and networks while maintaining data integrity and preventing unauthorized access.

2. Scope

This SOP applies to all personnel, contractors, and third-party vendors who require remote access to organizational systems and networks for support or maintenance purposes.

3. Definitions

Term	Definition
Remote Access	Connecting to an organization's systems or networks from a location outside of its physical premises.
Remote Support	Providing technical assistance or troubleshooting to users via remote access tools.
Multi-factor Authentication (MFA)	Authentication method requiring two or more verification factors.
Authorized User	An individual granted explicit permission to access remote systems for support purposes.

4. Responsibilities

- **IT Department:** Manage, monitor, and audit remote access activities; implement security measures.
- **Support Personnel:** Follow SOP protocols for secure remote sessions and data protection.
- **End Users:** Grant session access only to authorized support personnel and report suspicious activities.

5. Procedures

1. **Secure Authentication Methods**
   - All remote access must use **multi-factor authentication (MFA)**.
   - Passwords must comply with organizational security standards (minimum length, complexity, and expiration policy).
2. **Authorized User Access Protocols**
   - Remote access is restricted to authorized users as listed in the access control registry.
   - User permissions are reviewed and updated quarterly.
3. **Remote Session Initiation Guidelines**
   - All remote sessions must be pre-approved and scheduled when possible.
   - End users must be notified before session initiation and may be required to provide approval.
   - Use only organization-approved remote access tools (e.g., VPN, RDP, secure remote support applications).
4. **Data Protection Measures**
   - All session communications must be encrypted end-to-end.
   - No sensitive data should be downloaded or stored locally unless authorized and necessary for support.
   - Clipboard and file transfer features must be restricted and monitored where possible.
5. **Troubleshooting and Technical Support Process**
   - Issues must be documented in the support ticketing system with details of the action taken.
   - Follow escalation protocols for unresolved or critical incidents.
   - Obtain end-user confirmation upon resolution before closing the support session.
6. **Logging and Monitoring Activities**
   - All remote access sessions must be logged with timestamps, user details, and session duration.
   - Session recordings should be enabled where possible and stored securely for a minimum of 90 days.
   - Regular audits of access logs must be performed to detect unauthorized or suspicious activities.

6. Compliance and Review

- This SOP will be reviewed annually or as required by changes in technology or organizational policy.
- Non-compliance with these procedures may result in disciplinary action and/or revocation of remote access privileges.

7. References

- Information Security Policy
- Acceptable Use Policy
- Access Control Standards

8. Revision History

Version	Date	Description	Author
1.0	2024-06-15	Initial draft	IT Security Team