SOP: Troubleshooting Connectivity and Login Issues

This SOP provides a comprehensive guide for **troubleshooting connectivity and login issues**, covering common network problems, credential verification, system access protocols, and step-by-step resolution techniques. It aims to ensure seamless access to systems and applications by diagnosing and resolving connectivity disruptions and authentication failures efficiently.

1. Prerequisites

- Access to user account management tools/admin panel
- Basic knowledge of networking and authentication methods
- Authorized credentials for escalation if necessary

2. Issue Identification

1. Obtain detailed description of the issue from the user.
2. Determine if the problem is network-related or authentication-related:
    - Connectivity issues (e.g., can't access network resources, internet, VPN)
    - Login issues (e.g., incorrect password, account locked)

3. Troubleshooting Steps

3.1 Network Connectivity Issues

1. Ask the user to check physical connections (e.g., cables, Wi-Fi).
2. Verify network status/connection on the user's device.
3. Run network diagnostics (e.g., `ping`, `ipconfig/ifconfig`).
4. Check if other users or devices are affected.
5. Restart networking hardware (router/modem, if applicable).
6. Verify if any network maintenance/outages are ongoing.

3.2 Login Issues

1. Validate the user's credentials (username, password, domain).
2. Check for account lockout/disable status.
3. If password is forgotten or expired, guide user through password reset process.
4. Review authentication service availability (e.g., Active Directory, SSO providers).
5. Review recent security events/logs for suspicious activity.

4. Escalation Process

1. If unable to resolve:
    - Escalate the issue to IT Level 2/3 support.
    - Document all troubleshooting steps taken and findings.

5. Resolution and Follow-Up

1. Verify resolution by confirming user can connect and log in successfully.
2. Communicate resolution steps to user and provide documentation if needed.
3. Document the incident in the tracking system, noting root cause and steps taken.

6. Preventive Measures

- Educate users on secure login practices.
- Perform regular network health checks.
- Monitor system logs for recurring issues.
- Ensure password policies and backup procedures are enforced.

Note: Always adhere to your organization's IT security policies and privacy guidelines when troubleshooting user issues.