SOP: Repairing Domain Trust via PowerShell

Purpose
Fix ·The trust relationship between this workstation and the primary domain failed· without full domain r

Pre-Checks
- Local Admin Access: Log in with a local administrator account.
- Network Connectivity: Ensure device can reach a domain controller (VPN if remote).
- Time & DNS: Verify correct date/time and DNS points to enterprise DNS.
- AD Object: Confirm computer account exists and is enabled in Active Directory.

Steps
1. Open PowerShell as Administrator
   Start · Search · PowerShell · Right-click · Run as Administrator

2. Check Secure Channel Status
   Test-ComputerSecureChannel -Verbose
   Returns True = Trust OK
   Returns False = Trust Broken

3. Repair Trust
   Test-ComputerSecureChannel -Repair -Credential 'rush.edu\ENTACCOUNT'
   Enter rush.edu\ENTACCOUNT credentials when prompted.

4. Verify Repair
   Test-ComputerSecureChannel -Verbose
   Should return True after repair.

When to Use
- Device was offline for long periods (e.g., WFH without VPN).
- Restored from old snapshot or cloned without sysprep.
- AD computer account reset or disabled.
- Time/DNS issues corrected but trust still broken.

When NOT to Use
- No connectivity to AD (repair will fail).
- Azure AD-only devices (cloud join).
- Imaging failures due to DHCP/network issues·fix network first.
- Wrong machine identity (SID/OU mismatch)·requires full rejoin or re-image.

Alternatives
- Reset-ComputerMachinePassword or netdom reset (similar effect).
- Full domain leave/rejoin if AD object is corrupt or OU placement is wrong.