SOP: Remediation for MFA Re-Registration Token Conflict

Objective: Address and resolve issues caused by stale MFA tokens (ghost registrations) that interfere with re-registration in Microsoft Entra ID.

Root Cause:

When users re-register Microsoft Authenticator without removing prior registrations, the system may retain an obsolete token. This creates a 'ghost token' that can block new registration, confuse CA policy enforcement, or cause repeated prompts.

Resolution Steps:

1. Navigate to Microsoft Entra ID > Users > Select the affected user > Authentication Methods.
2. Remove all stale Microsoft Authenticator entries.
3. Also remove outdated phone numbers or FIDO2 keys if present.
4. Save changes and have the user sign in again. They will be prompted to register MFA from scratch.

PowerShell Cleanup (Admin Alternative):

Used when the UI is inaccessible or glitchy:

```
Connect-MgGraph -Scopes "UserAuthenticationMethod.ReadWrite.All" $user = Get-MgUser
-UserPrincipalName "username@domain.com" Get-MgUserAuthenticationMethod -UserId
$user.Id | Where-Object {$_.OdataType -eq
"#microsoft.graph.microsoftAuthenticatorAuthenticationMethod"} | ForEach-Object {
Remove-MgUserAuthenticationMethod -UserId $user.Id -AuthenticationMethodId $_.Id }
```

Recovery Using Temporary Access Pass (TAP):

If the user is locked out:
1. Admin generates a TAP (Temporary Access Pass).
2. User logs in using TAP.
3. MFA registration can be safely redone from scratch.

Governance Recommendations:

- Create SOPs for secure MFA re-registration workflows.
- Train helpdesk and IAM staff to recognize stale token behavior.
- Use Temporary Access Pass as part of the break-glass strategy.
- Regularly audit and clean up authentication methods via Entra reports.