



Privileged access hygiene checklist

Privileged accounts are how a bad day becomes a tenant-wide incident. Conditional Access and Secure Score point at the right direction; this checklist is what “good” looks like for the people who can change everything.

Use it for a New Zealand mid-market or public-sector Microsoft 365 tenant. Tick only what is enforced, not “planned”. Work top-down. Break-glass and emergency access first, then who holds standing admin, then phishing-resistant MFA, then just-in-time elevation (PIM), then monitoring.

Do not tighten Conditional Access on admins until at least one break-glass account exists, is excluded from lockout policies, and is monitored. Prefer Entra ID Privileged Identity Management (PIM) where you have P2 licensing. If you do not, keep standing privileged roles small, named, and reviewed on a hard cadence.

Document what you changed and why. That matters under Privacy Act 2020 when you need to show you take privileged access seriously.

BEFORE YOU START

- ☐ You know which licences you have (Entra ID P1 / P2) so you only tick PIM and Identity Protection items you can actually enforce
- ☐ At least one break-glass (emergency access) account strategy is agreed with whoever owns the tenant
- ☐ A named owner will review privileged roles on a cadence (not “when we get round to it”)

BREAK-GLASS AND EMERGENCY ACCESS

- ☐ At least two cloud-only break-glass accounts exist (no on-prem sync dependency)
- ☐ Break-glass accounts are excluded from Conditional Access policies that could lock out all admins
- ☐ Break-glass credentials are stored offline / in a sealed process, not in a shared mailbox
- ☐ Break-glass sign-in generates an alert the moment it is used
- ☐ Break-glass accounts are tested on a schedule (at least quarterly) and the test is recorded

STANDING PRIVILEGED ROLES

- ☐ Standing Global Administrators are kept small and named (aim for the minimum your operating model allows)
- ☐ Other highly privileged roles (Privileged Role Administrator, Security Administrator, Exchange Administrator, and similar) are inventoried — not left as “we think we know”
- ☐ Permanent standing admin is the exception; day-to-day work uses least privilege
- ☐ Shared admin accounts are gone; every privileged action maps to a person
- ☐ Unused or “just in case” privileged assignments are removed

PHISHING-RESISTANT MFA FOR ADMINS

- ☐ Privileged role sign-ins require phishing-resistant MFA where licensing and device support allow (passkeys / FIDO2 / certificate-based / Windows Hello for Business)
- ☐ Weak methods (SMS, voice, email OTP) are not accepted for privileged roles
- ☐ Security info registration for privileged users is hardened (separate Conditional Access; fresh interactive sign-in; managed device or trusted location where practical)

Privileged access hygiene checklist

- ☐ Temporary Access Pass or equivalent bootstrap is controlled — not a permanent back door

JUST-IN-TIME ELEVATION (PIM)

- ☐ Where Entra ID P2 is licensed, privileged roles use PIM eligible assignments rather than permanent active ones
- ☐ Activation requires MFA (phishing-resistant where you can), justification, and a short maximum duration
- ☐ Approval is required for the most sensitive roles (at least Global Administrator and Privileged Role Administrator)
- ☐ Eligible assignments are reviewed; unused eligibility is removed
- ☐ If you do not have P2 yet, standing privileged roles still have a named owner and a fixed review date

DEVICES AND SESSIONS

- ☐ Privileged role access prefers managed / compliant devices where Intune licensing allows
- ☐ Persistent browser sessions for privileged roles are limited or blocked
- ☐ Privileged work is not done from unmanaged personal browsers as the default path
- ☐ Admin portals and Graph-heavy tools are in scope for Conditional Access — not left on “All cloud apps” hope

MONITORING AND RESPONSE

- ☐ Privileged role activation, assignment changes, and break-glass sign-ins are in an alert queue with a named owner
- ☐ Directory Audit and Sign-in logs for privileged accounts are retained and reviewed after incidents
- ☐ A simple response path exists: disable or revoke sessions, remove attacker MFA methods, re-enable only after verification
- ☐ After any Entra / identity disclosure or major admin change, privileged hygiene is reviewed on purpose

OPERATING RHYTHM

- ☐ Privileged role inventory is reviewed at least quarterly
- ☐ Exclusions from Conditional Access (including break-glass) are listed and reviewed on the same cadence
- ☐ Changes are recorded: what was switched on, who approved it, and why
- ☐ New admins get a short privileged-access briefing before their first elevation

What good looks like: you can name every standing Global Administrator. Break-glass is boring, tested, and noisy when used. Day-to-day privileged work is just-in-time, phishing-resistant, and on a managed device where you can. And if Microsoft publishes another identity advisory tomorrow, you already know who can change the tenant — and how they prove it.