Tech 04 — Admin Console Security (Azure)

Summary

We secure admin access without Premium features by enabling Security Defaults, enforcing per-user MFA for admins, and requiring modern authentication. Legacy/basic protocols (POP/IMAP/SMTP AUTH) are disabled. Admin roles follow least privilege and are reviewed quarterly; no break-glass accounts.

Implemented Controls

- Security Defaults enabled tenant-wide (enforces MFA for admins; blocks legacy/basic auth).
- Modern authentication required for Exchange Online; basic authentication blocked.
- Per-user MFA enforced for admin accounts.
- Least privilege for admin roles; quarterly access review recorded.

Evidence — Screenshot paths

- Security Defaults enabled: `answers/evidence/admin-security/security-defaults-enabled-2025-10-17.png`
- Microsoft 365 Modern authentication ON; legacy protocols OFF: `answers/evidence/admin-security/m365-modern-aut`
- Per-user MFA "Enforced" for admin: `answers/evidence/admin-security/per-user-mfa-enforced-2025-10-17.png`
- Optional: Admin role assignments: `answers/evidence/admin-security/admin-role-assignments-2025-10-17.png`
- Optional: Admin sign-in logs show MFA: `answers/evidence/admin-security/admin-signin-logs-mfa-2025-10-17.p`

Onsite Verification (click path)

- Entra ID → Properties → Manage security defaults → shows "Enabled".
- Microsoft 365 admin center → Settings → Org settings → Modern authentication → shows modern auth ON and basic auth blocked.
- Entra ID → Users → Per-user MFA → Multi-Factor Authentication portal → admin accounts show Status "Enforced".

ISO 27001 Mapping

- A.5.15 Access control, A.8.3 Secure authentication, A.5.18 Access rights, A.8.16 Monitoring activities.