

IT PARTNER LLC

Microsoft 365 Security & Compliance Assessment

Sample Client (Regulated Multi-State Retail Group)

Detailed findings, verification results and remediation roadmap

Prepared for	Sample Client (Regulated Multi-State Retail Group)
Primary tenant domain	██████████.com
Prepared by	Mike Mackey, Microsoft 365 Security Practice, IT Partner LLC
Assessment collected	2 September 2026
Verification completed	3 September 2026
Report date / version	3 September 2026 · v1.0
Classification	SAMPLE DELIVERABLE — client identifiers redacted

This document contains security findings about a live production environment. Distribution should be limited to the client's leadership, IT and legal stakeholders and their designated advisors.

Contents

1. Executive Summary	4
1.1 Headline numbers	4
1.2 What matters most	4
1.3 The structural constraint	5
1.4 Recommended path	5
2. Scope, Method and Verification	6
2.1 Scope	6
2.2 Method	6
2.3 Severity ratings	6
2.4 Confidence	6
3. Tenant Profile	8
3.1 Identity	8
3.2 Population	8
3.3 Domain estate	8
3.4 Licensing	9
4. Security Posture Overview	10
4.1 Microsoft Secure Score	10
4.2 Compliance Manager	10
4.3 Pattern across the estate	10
5. Detailed Findings	11
5.1 Identity & Access	11
5.2 Email Security	15
5.3 Endpoint Security	18
5.4 Collaboration & Sharing	20
5.5 Data Protection & Compliance	22
5.6 Tenant Hygiene	24
6. What Is Working	25
7. Licensing: The Structural Constraint and Recommendation	26
7.1 Options	26
8. Acquisition Onboarding Security Baseline	27
9. Remediation Roadmap	28
Phase 0 — Stabilise (Weeks 1–2)	28
Phase 1 — Harden (Days 15–60)	28
Phase 2 — Govern (Days 60–120)	29
Phase 3 — Sustain (Ongoing)	30

Success measures 30

Appendix A. Findings Register 31

Appendix B. Email Authentication by Domain (verified 3 Sep 2026) 33

Appendix C. Conditional Access and Privileged Roles 35

 C.1 Conditional Access policies (verified detail) 35

 C.2 Directory role assignments (all permanent; no PIM eligibility)..... 35

Appendix D. Verification Log and Scope Exclusions 36

 D.1 Items flagged for verification after portal collection 36

 D.2 Not assessed 36

 D.3 Evidence package 37

1. Executive Summary

IT Partner LLC performed a read-only security and compliance assessment of the Sample Client (Regulated Multi-State Retail Group) Microsoft 365 tenant on 2 September 2026, followed by a verification pass on 3 September 2026 using Microsoft Graph, Exchange Online and Security & Compliance PowerShell together with external DNS checks of all 35 accepted domains. The tenant serves 792 identities, 622 mailboxes and 35 domains across a multi-state, regulated cannabis retail group and its investment holding entity, which is actively acquiring further businesses and locations.

The overall picture is consistent and can be stated plainly: Microsoft's default and preset protections have been adopted well, and almost nothing beyond them has been configured. Detection is largely on. Prevention, data governance and configuration management are largely absent. Microsoft Secure Score stands at 52.7% and Compliance Manager at 60%, both in the bottom half of comparable organisations.

The assessment raised **32 findings — 8 Critical, 13 High, 8 Medium and 3 Low**. Twelve controls were found to be correctly configured and are credited in Section 6. Every finding in this report was either observed directly in the administrative portals or verified through PowerShell and DNS; where a residual uncertainty remains it is stated on the finding itself.

1.1 Headline numbers

Metric	Value	Context
Microsoft Secure Score	52.7%	623 of 1,182 points; Device category 45.3%
Compliance Manager posture	60%	Rated Moderate; no industry assessments
Findings	32	8 Critical · 13 High · 8 Medium · 3 Low
Identities / mailboxes / guests	792 / 622 / 143	574 enabled members, 75 disabled, 143 guests
Identities unable to perform MFA	174 (24%)	Only Email OTP enabled in the modern policy
Accepted domains without DKIM	34 of 35	21 have no DMARC record at all
Managed endpoints	21	vs. 622 mailboxes; 0 AV / ASR / BitLocker / firewall policies
Sensitivity labels / retention policies / holds	0 / 0 / 0	3 eDiscovery cases open with no holds
Stale enabled accounts (90+ days)	190	87 have never signed in
Users flagged at risk (unremediated)	16	including one Global Administrator

1.2 What matters most

Five issues account for most of the risk, and the first three can be closed in days at no licence cost:

Finding(s)	Why it matters
C-8 / C-3	A Global Administrator account is currently flagged at risk by Identity Protection and unremediated, while the modern authentication policy has every strong MFA method disabled with only Email OTP enabled and a migration in progress that would leave the organisation without working MFA if it completed today.

Finding(s)	Why it matters
C-2	Email from 34 of 35 brand and corporate domains cannot be authenticated: DKIM has never been enabled and 21 domains have no DMARC record at all. Customers, patients, banks, regulators and outside counsel cannot distinguish genuine mail from forged mail, and impersonation attempts have already been observed.
C-7 / C-6	Three eDiscovery cases are open — one apparently involving litigation — yet no mailbox in the tenant is under any hold, and there is no retention policy, sensitivity label or custom DLP policy anywhere. Preservation depends on users not deleting things.
C-1 / H-1 / H-8	Every external-sharing control is at its most permissive setting and they compound: anyone can invite any guest (143 exist, 112 inactive), the default share link is anonymous, editable and permanent, and unmanaged devices have full access with sessions that never expire.
C-5 / H-5 / H-6	Endpoints are running on Windows defaults: no attack-surface-reduction, antivirus, BitLocker or firewall policy, every user a local administrator, no LAPS, and 17 previously-satisfied controls have silently regressed. Defender would see a ransomware intrusion; very little is configured to stop one.

1.3 The structural constraint

Verification of licence service plans confirms that 365 of roughly 560 licensed users hold Business Basic or Business Standard, which include no Entra ID P1, Intune or Defender for Office 365 entitlement. Only 195 users (Business Premium and E5) can be covered by Conditional Access, device management and advanced email protection. This is the most likely explanation for the 174 identities that cannot perform MFA, the 21-device management footprint and the absence of device-based access control, and it means several remediations in this report cannot be applied tenant-wide until the licensing question is decided (Section 7).

1.4 Recommended path

The roadmap in Section 9 is organised in four phases. Phase 0 (weeks 1–2) closes the gaps an attacker would use this month — the risky administrator, MFA methods, holds, DKIM/DMARC, sharing defaults, forwarding, the filtering bypass, impersonation protection and ASR rules — with configuration changes only. Phase 1 (to day 60) takes the licensing decision and makes identity, device and collaboration controls enforceable. Phase 2 (to day 120) builds the data-protection layer a regulated operator needs. Phase 3 establishes the operating rhythm and an acquisition onboarding baseline so that each future tenant-to-tenant migration lands securely rather than adding to the backlog.

Bottom line

The tenant is not neglected, but it is undefended beyond Microsoft's defaults. The highest-consequence items are inexpensive and fast to fix; the durable fix requires a licensing decision. IT Partner LLC recommends starting Phase 0 immediately and taking the licensing decision within 30 days.

2. Scope, Method and Verification

2.1 Scope

The assessment covered the Microsoft 365 tenant only: Microsoft Entra ID (identity, Conditional Access, authentication methods, privileged roles, application consent, device settings), Microsoft Defender (Secure Score, Defender for Office 365, Defender for Endpoint, email authentication), Exchange Online (mail flow, sharing, forwarding), SharePoint Online, OneDrive and Teams (external sharing and federation), Microsoft Intune (compliance, configuration and endpoint security policies) and Microsoft Purview (DLP, labels, retention, audit, eDiscovery, Compliance Manager). On-premises Active Directory and non-Microsoft systems were out of scope; see Appendix D for the list of items not assessed.

2.2 Method

Collection on 2 September 2026 was performed read-only through the Entra, Defender, Purview, Exchange, SharePoint, Teams, Intune and Microsoft 365 administrative portals using the delegated administrative account. No policy, setting or configuration was created, modified, enabled, disabled or saved. Where a settings wizard had to be opened to read a value it was cancelled without saving.

On 3 September 2026 a second, read-only pass collected machine-readable data with Microsoft Graph PowerShell (Conditional Access, authorisation and authentication-method policies, role assignments, PIM, licence service plans, sign-in activity, risky users, OAuth grants, Intune policies, domains), Exchange Online PowerShell (transport rules, DKIM, outbound spam, remote domains, sharing policies, mailbox hold/archive/audit/forwarding state) and Security & Compliance PowerShell (retention, labels, DLP, audit retention, eDiscovery cases and holds). SPF, DKIM selector and DMARC records for all 35 domains were checked by external DNS lookup.

2.3 Severity ratings

Severity	Meaning
Critical	Exploitable now with high likelihood and high impact, or a control failure that removes a fundamental protection (e.g., MFA, preservation, email authentication). Fix within two weeks.
High	A significant weakness that materially lowers the cost of a successful attack or breaches a widely-accepted baseline. Fix within 60 days.
Medium	A weakness that increases exposure or would be flagged in an audit; fix within 120 days or as part of a related project.
Low	Hygiene, cost or clarity issues with limited direct security impact.

Ratings are the assessor's judgement against the CIS Microsoft 365 Foundations Benchmark v4 and Microsoft's published baselines. They are not a quantified risk score. Where the CIS control is known it is cited on the finding.

2.4 Confidence

Each finding carries a verification status. "Verified" means the underlying configuration was confirmed by PowerShell/Graph export or DNS on 3 September 2026 in addition to the portal observation. Items that remain partially unverified are limited to: the contents of the custom user-consent policy, site-level holds inside the two

Premium eDiscovery cases, the identities behind the 46 OAuth grants, and which parked domains the client intends to keep. None of these change a severity rating.

3. Tenant Profile

3.1 Identity

Tenant	Sample Client (Regulated Multi-State Retail Group)
Tenant ID	██████████-████-████-████-████████████████
Primary domain	██████████.com
Initial domain	██████████.onmicrosoft.com
Region / data residency	United States
Industry context	Multi-state regulated cannabis retail (dispensary brands) with an investment holding entity; actively acquiring businesses and locations (one tenant-to-tenant migration completed, further migrations in planning)
Security defaults	Disabled (Conditional Access in use)
Technical contact / privacy contact	Set / Not set

3.2 Population

Metric	Count	Note
Directory identities	792	574 enabled members, 75 disabled members, 143 guests
Enabled members with no sign-in in 90+ days	190	161 beyond 180 days; 87 never signed in
Guest accounts	143	62 never signed in; 50 inactive 90+ days
Exchange mailboxes	622	534 user, 88 shared; 6 with online archive
MFA-capable identities	543 of 717	174 cannot perform MFA; 58 passwordless-capable
Users flagged at risk (unremediated)	16	Includes one Global Administrator
Managed endpoints (Intune + Defender)	21	All Windows; 17 workgroup-joined, 4 Entra-joined
Accepted domains	35	14 carry user accounts; 21 carry 0–1
Privileged role holders	4	3 Global Administrators; 24 permanent role assignments
Enterprise applications / OAuth grants	695 / 46	33 tenant-wide grants; 5 app registrations

3.3 Domain estate

Thirty-five accepted domains span the dispensary brands (a national brand plus eleven state-specific variants, and several regional brands), the corporate and holding entities, and a set of consumer and legacy domains. Fourteen domains carry user accounts; the remaining twenty-one carry at most one and appear to be parked, defensive or legacy. The primary domain was recently migrated from a legacy corporate domain, and residue from a previous tenant migration is still visible in DNS and mail-flow rules (L-2). Appendix B lists every domain with its verified email-authentication state.

3.4 Licensing

Product	Assigned	Purchased	Entra P1/P2	Intune	Defender for Office
Microsoft 365 Business Standard	194	199	No	No	No
Microsoft 365 Business Basic	171	175	No	No	No
Microsoft 365 Business Premium	168	177	Yes (P1)	Yes	Yes (P1)
Microsoft 365 E5	27	30	Yes (P2)	Yes	Yes (P2)
Exchange Online Plan 2	8	14	No	No	No
Power BI Pro	41	43	—	—	—
Power BI Premium Per User	5	5	—	—	—
Planner Plan 1	6	7	—	—	—
Teams Phone / Calling Plan	4	5	—	—	—
Visio Plan 1	2	3	—	—	—
Microsoft 365 Copilot (dept.)	2	2	—	—	—

Verified 3 Sep 2026 from Get-MgSubscribedSku service plans: Business Basic and Business Standard carry no AAD_PREMIUM, INTUNE_A or ATP_ENTERPRISE service plan. 365 of ~560 licensed users therefore have no Entra ID P1 (Conditional Access), no Intune and no Defender for Office 365 entitlement. 195 users (Business Premium + E5) do.

4. Security Posture Overview

4.1 Microsoft Secure Score

Measure	Value
Overall score	52.73% (623.22 of 1182 points)
Apps	81.82%
Identity	66.73%
Data	55.56%
Device	45.34%
Actions to address	114
Regressed actions	17
Planned / Risk accepted	0 / 0

Device is the weakest category by a wide margin and dominates the opportunity list: the top nineteen recommended actions are all Attack Surface Reduction rules behind a single Intune policy that does not exist (C-5). The seventeen regressed actions matter more than the raw score — they show previously-satisfied endpoint controls drifting back off. Nothing is marked Planned or Risk-accepted, so the backlog has never been triaged.

4.2 Compliance Manager

Compliance Manager reports a posture score of 60% (Moderate) against the Microsoft 365 baseline, 61% for data protection and 63% for AI. No industry-specific assessment (for example NIST CSF, PCI DSS or a state cannabis record-keeping template) has been instantiated, so the score reflects generic controls only.

4.3 Pattern across the estate

Layer	Detection / defaults	Prevention / configuration
Email	Standard preset on for all recipients; TABL maintained	No DKIM/DMARC; impersonation list 1/350; auto-forward allowed; SCL -1 bypass rule
Identity	Admin MFA complete; legacy auth blocked; risk detections firing	Only Email OTP enabled; risky GA unremediated; no PIM; no break-glass; open app/tenant creation
Endpoint	Defender onboarded on 21/21; EDR profile works	No ASR / AV / BitLocker / firewall / baseline; everyone local admin; 17 regressions
Collaboration	Modern-auth-only enforced in SharePoint	Anonymous edit links by default; open guest invites; open Teams federation; full unmanaged access
Data & compliance	Audit log on; mailbox auditing on all mailboxes; eDiscovery in use	No labels, retention, DLP or holds; 6 archives; Lockbox off

5. Detailed Findings

Findings are grouped by domain and ordered by severity within each group. Each carries a verification status, an effort estimate (S = under a day, M = one to five days, L = a project of two or more weeks) and the roadmap phase in which it is scheduled.

5.1 Identity & Access

C-3 · Every strong MFA method is disabled in the Authentication methods policy; only Email OTP is enabled

CRITICAL	Effort S · Phase 0 · Verified (Graph, 3 Sep 2026)	CIS 5.2.3.1–5.2.3.4
----------	---	---------------------

Observation. Passkey/FIDO2, Microsoft Authenticator, SMS, Temporary Access Pass, OATH tokens, voice and certificate-based authentication are all disabled. Email OTP alone is enabled. Migration from the legacy per-user MFA policy is 'in progress'.

Verified via Graph (PolicyMigrationState = migrationInProgress). MFA today is served by the deprecated legacy per-user MFA/SSPR configuration, which Microsoft retired on 30 September 2025 and is on a Microsoft-driven retirement path. In the modern policy that will replace it, the only enabled method is Email OTP — a factor delivered to the same mailbox an attacker is trying to reach, and one Microsoft does not consider suitable as a primary MFA method for members. If the migration completes in this state the organisation loses working MFA. The Authenticator registration campaign targets all users but nudges them toward a method that is disabled.

Impact. Scheduled loss of MFA for the entire organisation; no phishing-resistant option available to administrators.

Recommendation. Immediately enable Microsoft Authenticator (push + passwordless, number matching on), Passkeys (FIDO2) and Temporary Access Pass in the Authentication methods policy; leave SMS/voice disabled or restrict to a legacy group; then complete the migration to the unified policy and disable Email OTP for members. Issue passkeys or Windows Hello for Business to all privileged accounts.

Evidence: X-AuthenticationMethodsPolicy.json; raw/12-entra-identity.json

C-4 · 174 of 717 identities (24%) cannot perform MFA; 365 users have no Conditional Access entitlement

CRITICAL	Effort M · Phase 1 · Verified (Graph + SKU service plans, 3 Sep 2026)	CIS 5.2.2.2
----------	---	-------------

Observation. The customer 'MFA' Conditional Access policy correctly targets all users and all apps (verified), but 174 identities have no registered second factor and 92% cannot use passwordless. Licensing verification shows 365 Business Basic/Standard users hold no Entra ID P1 service plan.

Verified: the MFA policy includes All users / All applications with three excluded accounts; the Block legacy authentication policy is likewise tenant-wide. The gap is therefore registration and licensing, not policy scope. Business Basic and Business Standard SKUs carry no AAD_PREMIUM service plan, so Conditional Access is not licensed for ~365 users even though the policy technically evaluates them; Microsoft's licensing terms require every user benefiting from CA to hold P1. Administrative accounts are fully covered (Secure Score 10/10).

Impact. A quarter of the organisation can be compromised with a password alone; tenant-wide CA is out of licensing compliance.

Recommendation. Run a registration campaign with a deadline and enforce via CA 'require MFA registration' for the 174 users; block sign-in for stale accounts (H-12) first to shrink the population. Resolve the licensing gap (Section 7) — either uplift Business Basic/Standard users to Business Premium or add Entra ID P1 — before extending CA further. Review the three exclusions on the MFA policy and replace them with dedicated break-glass accounts (H-13).

Evidence: V1-ConditionalAccessPolicies.json; V2-SubscribedSkus.json; raw/14-users-and-admins.json

C-8 · A Global Administrator is flagged at risk (medium) and 15 other risky users are unremediated

CRITICAL	Effort S · Phase 0 · Verified (Graph, 3 Sep 2026)	CIS 5.2.2.6, 5.2.2.7
----------	---	----------------------

Observation. Identity Protection shows 16 users in the atRisk state (3 medium, 13 low), including Global Administrator [REDACTED]@[REDACTED].com — risk last updated 2 September 2026, the day of the assessment. Some low-risk flags date back to 2023 and have never been reviewed.

No customer user-risk or sign-in-risk policy exists (Secure Score 0/7 and 0.27/7); the Microsoft-managed risky sign-in policy applies to a single group and only to High-risk sign-ins. A Global Administrator with an unremediated risk flag, permanent role assignment, no phishing-resistant MFA requirement (the baseline policy is report-only) and universal local-admin rights on Entra-joined devices (H-6) is the single highest-consequence identity in the tenant.

Impact. Potential ongoing compromise of a Global Administrator account; no automated response to risky behaviour anywhere in the tenant.

Recommendation. Today: investigate the GA account's risk detections and sign-in logs, reset its password, revoke sessions and register a passkey; then triage all 16 at-risk users (confirm compromised or dismiss with justification). Phase 1: create Conditional Access policies — block High user risk, require MFA + password change on Medium user risk, require MFA on Medium/High sign-in risk — for all licensed users (Entra P2 is available to the 27 E5 users; extend as licensing allows).

Evidence: X-RiskyUsers.json; V1-ConditionalAccessPolicies.json

H-3 · Admin-portal MFA and phishing-resistant admin MFA policies are Report-only; the risky sign-in policy covers one group

HIGH	Effort M · Phase 1 · Verified (Graph, 3 Sep 2026)	CIS 5.2.2.1, 5.2.2.3
------	---	----------------------

Observation. Verified policy detail: two of five Conditional Access policies enforce nothing. The Microsoft-managed admin-portal MFA policy (14 roles) and the Baseline Security Mode phishing-resistant admin MFA policy (19 roles, created 20 Jul 2026) are both report-only. The risky sign-in policy targets a single group and High risk only.

Only two customer-authored policies exist (MFA, Block legacy auth) for a 622-mailbox, 35-domain, multi-state organisation. There is no device-compliance policy, no location or session control, no separate policy set for privileged roles, and no sign-in frequency for admins. Baseline security mode is present but 'automatically apply' is unchecked with 0 policies applied.

Impact. Administrators are not required to use phishing-resistant MFA; admin portals can be reached with a phishable factor.

Recommendation. Enforce the phishing-resistant admin MFA policy once passkeys are issued (C-3), enforce admin-portal MFA, and build the standard policy set: require compliant device for all apps (after H-4), block unknown platforms, sign-in frequency 1 hour with no persistent browser for admins, block access from countries the business does not operate in, and require MFA for guests. Use report-only for 7 days per policy before enforcing.

Evidence: V1-ConditionalAccessPolicies.json

H-10 · Standard users can register applications, create tenants and read their own BitLocker keys; user consent runs on a custom policy

HIGH	Effort S · Phase 1 · Verified (Graph, 3 Sep 2026); consent policy contents unverified	CIS 5.1.2.x, 5.1.5.1
------	---	----------------------

Observation. Verified authorization policy: AllowedToCreateApps = true, AllowedToCreateTenants = true, AllowedToReadBitlockerKeysForOwnedDevice = true, AllowEmailVerifiedUsersToJoinOrganization = true. Entra admin center is not restricted. User consent is governed by a custom permission-grant policy ('rm-consent-policy-v1') rather than one of Microsoft's standard settings.

App registration by any user is a common OAuth-consent phishing and persistence path. Tenant creation by any user places data entirely outside governance. The custom consent policy's contents could not be retrieved and its effective behaviour is unknown. On the positive side, the admin consent workflow is enabled with a reviewer, notifications and a 30-day expiry (single reviewer is a bus-factor risk).

Impact. Persistence and data-access paths that bypass MFA and Conditional Access entirely.

Recommendation. Set users can register applications = No; restrict non-admin tenant creation = Yes; restrict Entra admin center access; disable email-verified self-service join; set user consent to 'Allow user consent for apps from verified publishers for selected permissions' (low-impact only) or disable it; add a second consent reviewer; disable user BitLocker key self-recovery.

Evidence: V5-AuthorizationPolicy.json; V5-AdminConsentRequestPolicy.json

H-11 · 190 enabled accounts have not signed in for 90+ days (87 never); each is a licensed, MFA-less attack surface

HIGH	Effort M · Phase 1 · Verified (Graph, 3 Sep 2026)	CIS 1.1.4
------	---	-----------

Observation. Verified from sign-in activity: of 574 enabled member accounts, 190 have no sign-in in 90 days (161 beyond 180 days) and 87 have never signed in at all. 75 accounts are already disabled.

Dormant accounts are the population least likely to have registered MFA (C-4) and the most likely to carry a weak or reused password from a store onboarding. They consume licenses (35 seats sit unassigned while ~190 are assigned to dormant accounts), and in a high-turnover retail workforce they accumulate continuously without a joiner-mover-leaver process. 88 shared mailboxes exist; whether their sign-in is blocked was not captured.

Impact. Large, unmonitored credential surface; license waste; leaver access not revoked.

Recommendation. Block sign-in and revoke sessions for the 87 never-used and 161 >180-day accounts after manager confirmation; convert leavers to shared mailboxes with sign-in blocked, or delete after retention; block sign-in on all shared mailboxes; implement a leaver checklist and a monthly inactive-account report (Entra

inactive user recommendation or a scheduled Graph script); reclaim the licenses toward the Business Premium uplift.

Evidence: X-AllUsers-SignInActivity.json; X-Mailboxes-HoldAuditArchive.json

H-12 · No emergency-access (break-glass) account; all 24 privileged role assignments are permanent; PIM unused despite P2 entitlement

HIGH	Effort M · Phase 1 · Verified (Graph, 3 Sep 2026)	CIS 5.1.1.1, 5.3.1, 5.3.2
-------------	---	---------------------------

Observation. Verified: 24 active directory-role assignments across 4 people, all 'Assigned' with no end date; zero PIM eligible assignments. All three Global Administrators are in daily use (last sign-in 2 Sep 2026); none is a dedicated, CA-excluded emergency access account. Azure resource elevated access is enabled with the portal flagging 2 users.

Two internal administrators hold Global Administrator plus eight to eleven additional roles each; a third holds Exchange, User and Global Reader roles. The 27 E5 licenses include Entra ID P2, so Privileged Identity Management is available and unused. If the MFA policy's three excluded accounts are not break-glass accounts, a Conditional Access misconfiguration could lock every administrator out of the tenant.

Impact. Standing privilege for every admin, no just-in-time approval or audit, and no recovery path from a CA lockout.

Recommendation. Create two cloud-only break-glass accounts with 64-character passwords or FIDO2 keys stored offline, excluded from all CA policies and monitored by an alert on any sign-in; move all privileged roles to PIM eligible assignments (max 8-hour activation, MFA and justification required); reduce Global Administrator to 2 plus break-glass and use least-privilege roles for daily work; remove Azure elevated access from the [REDACTED] account; separate the IT Partner administrative account from customer accounts via GDAP where possible.

Evidence: V6-RoleAssignments-Active.json; V6-PIM-ActiveAssignments.json; V6-GlobalAdmins-Detail.json; raw/01-entra-tenant-properties.json

M-5 · On-premises password protection is in Audit mode; no custom banned-password list; on-premises AD is unassessed

MEDIUM	Effort S · Phase 1 · Verified (portal)	CIS 5.2.3.x
---------------	--	-------------

Observation. Password protection for Windows Server AD is deployed but in Audit rather than Enforced mode, and the custom banned list is empty. Secure Score items for LDAP signing (0/7), LDAP encryption (0/7), NTLM (0/8), LM authentication level (0/8) and Defender for Identity sensors (0/5) indicate domain controllers exist and are unmonitored.

Weak passwords are being observed rather than blocked; brand and locality terms ('natures', 'medicines', 'dispensary', city names) are not banned. The on-premises environment was out of scope for this assessment.

Impact. Weak passwords on synchronised accounts; unsigned LDAP and permitted NTLM are classic relay conditions.

Recommendation. Switch password protection to Enforced; add ~50 brand, product and locality terms to the banned list; commission a separate on-premises Active Directory assessment and deploy Defender for Identity sensors (included in E5, 27 seats).

Evidence: raw/12-entra-identity.json; raw/03-secure-score-actions.csv

M-6 · 46 OAuth permission grants (33 tenant-wide) including mail, files and full site control are not inventoried

MEDIUM	Effort S · Phase 1 · Verified — counts (Graph); app identities unresolved	CIS 5.1.2.2
---------------	---	-------------

Observation. Verified: 46 delegated OAuth grants exist across 695 enterprise applications; 33 are tenant-wide (admin-consented) and include scopes such as Mail.ReadWrite, Mail.Send, Files.ReadWrite.All, Sites.FullControl.All and Directory.Read.All. Five app registrations exist (two created May–June 2026 for AI projects). Application names could not be resolved in this export.

Some of these will be Microsoft first-party and legitimate; others may be third-party SaaS with standing access to every mailbox and every file. No review process exists, and users can register their own apps (H-10).

Impact. Unknown third parties may hold persistent, MFA-independent access to mail and files.

Recommendation. Export enterprise applications with their permission grants (Entra → Enterprise apps → Permissions, or Defender for Cloud Apps OAuth app governance); remove unrecognised tenant-wide grants; review the two 2026 AI app registrations for credentials and scopes; enable app governance alerts.

Evidence: X-OAuthGrants.json; X-AppRegistrations.json

M-8 · Device registration is unrestricted: any user may join up to 50 devices with no MFA required

MEDIUM	Effort S · Phase 1 · Verified (portal)	CIS 5.1.x
---------------	--	-----------

Observation. Users may join and register devices = All; MFA to register or join = No; maximum devices per user = 50.

Combined with H-6 (registering user becomes local admin) an attacker with a phished password can register a device, gain a device identity and bypass device-based controls.

Impact. Weak device-identity trust; device-based Conditional Access can be gamed.

Recommendation. Require MFA to register or join devices; reduce maximum devices to 5–10; restrict device join to a group or use Autopilot enrolment only.

Evidence: raw/12-entra-identity.json

5.2 Email Security

C-2 · DKIM is disabled on 34 of 35 domains and DMARC is absent on 21; every brand domain is spoofable

CRITICAL	Effort M · Phase 0 · Verified (portal 2 Sep + external DNS 3 Sep 2026)	CIS 2.1.9, 2.1.10
-----------------	--	-------------------

Observation. DKIM signing has never been enabled for 34 accepted domains including the primary domain ██████████.com. External DNS verification (3 Sep 2026) shows 21 domains have no DMARC record, 7 are at p=none, and only 7 enforce (5 quarantine, 2 reject) — on SPF alignment alone.

Verified externally: SPF exists on 34 of 35 domains (mostly hard-fail, a positive), but DKIM is unsigned everywhere except ██████████.org — which in turn has no SPF record at all. The 7 enforcing DMARC domains rely solely on SPF, which breaks on forwarded mail and any third-party sender. ██████████.com carries DKIM CNAME records pointing at a different tenant (█████████.com) — a residue of a previous tenant migration that would silently break signing if enabled. Most DMARC records carry no reporting (rua) address, so

nobody sees abuse. Defender recorded one impersonation detection in the week before assessment and a manually-blocked impersonation attempt targeting a named executive.

Impact. Attackers can send mail that appears to originate from any dispensary brand, the investment entity or the corporate domain to customers, patients, banks, regulators and outside counsel, and receiving systems have no reliable signal to reject it. The victims are external, so the brand damage is too.

Recommendation. Phase 0: publish and enable DKIM (2048-bit) for the 14 user-carrying domains starting with [REDACTED].com; correct the [REDACTED].com selector CNAMEs to this tenant; add SPF to [REDACTED].org; publish DMARC p=none with a rua mailbox on all 35 domains. Phase 1: move user-carrying domains to p=quarantine then p=reject; set parked domains to p=reject with SPF '-all' and a null MX. Add DMARC reporting (Microsoft or a DMARC analytics service).

Evidence: raw/06-email-authentication-dkim.json; dns_verification.csv

H-7 · Impersonation protection covers 1 user and 0 of 35 domains, with impersonation attempts already observed

HIGH	Effort S · Phase 0 · Verified (portal, 2 Sep 2026)	CIS 2.1.7
-------------	--	-----------

Observation. Of 350 available protected-user slots, 1 is used; of 50 protected-domain slots, 0. Defender reported 1 impersonation detection in the prior 7 days and the Tenant Allow/Block List contains a manually-blocked sender described as a 'fake email with [executive] name'.

The Standard preset is correctly applied to all recipients (a genuine positive), but it protects only what it is told about. For an organisation with an investment arm, executive and finance-team impersonation is the highest-yield business email compromise vector; the control designed to stop it is 1/350 configured.

Impact. CEO/CFO fraud, payroll diversion and vendor-payment redirection are not specifically defended.

Recommendation. Add all executives, finance, HR, and store/regional managers to protected users; add all 35 owned domains plus key counterparties (counsel, accountants, banks, POS/seed-to-sale vendors) to protected domains; enable mailbox intelligence impersonation protection actions = Quarantine; designate Priority accounts for executives; turn on user-reported message settings and spam-policy admin notifications.

Evidence: raw/04-defender-office-policies.json

H-9 · External auto-forwarding is not blocked by policy

HIGH	Effort S · Phase 0 · Verified (Exchange PowerShell, 3 Sep 2026)	CIS 6.2.1
-------------	---	-----------

Observation. Verified: the outbound spam policy AutoForwardingMode is 'Automatic' and the default remote domain has AutoForwardEnabled = true. Secure Score confirms 'Ensure all forms of mail forwarding are blocked' at 0/5. 33 mailboxes currently forward — all to internal addresses — and 0 external auto-forwards occurred in the prior 7 days.

The absence of external forwarding today is good hygiene, not a control. An attacker who phishes one mailbox (24% of users have no MFA) can silently forward all mail externally — the most common persistence step in business email compromise.

Impact. Silent exfiltration channel available to any compromised mailbox.

Recommendation. Set outbound spam policy AutoForwardingMode to Off; set remote domain AutoForwardEnabled to false; add a transport rule to reject auto-forwards to external domains with an explanatory NDR; review the 33 internal forwards for leavers and shared-mailbox sprawl.

Evidence: X-OutboundSpamPolicy.json; X-RemoteDomains.json

H-13 · A transport rule sets SCL –1 for any sender claiming a █████.com domain — a spoofable filtering bypass

HIGH	Effort S · Phase 0 · Verified (Exchange PowerShell, 3 Sep 2026)	CIS 2.1.x
------	---	-----------

Observation. Verified rule contents: 'Whitelist █████.com' (priority 0, enabled, fired within 2 hours of capture) sets the spam confidence level to –1 whenever the sender's address domain is █████.com, track.█████.com, reply.█████.com or notify.█████.com. The condition checks the claimed sender domain only — not authentication results.

Any phishing message with a forged █████.com From address walks past spam, phishing and bulk filtering. Box is a common lure for credential-phishing ('a document has been shared with you'). Safe Links/Safe Attachments still apply, but the message reaches the inbox with no spam verdict.

Impact. High-confidence phishing bypass reachable by anyone who can forge a From header.

Recommendation. Delete the rule. If █████.com notifications are genuinely mis-filtered, add █████.com to the anti-spam policy's allowed sender domains only with the additional condition that the message passed DMARC/authentication (Authentication-Results header contains 'dmarc=pass'), or use the Tenant Allow/Block List with a justified expiry.

Evidence: V4-TransportRules.json

M-4 · E-signature BCC rule is undocumented and references legacy-tenant addresses

MEDIUM	Effort S · Phase 1 · Verified (Exchange PowerShell, 3 Sep 2026)	—
--------	---	---

Observation. Verified rule contents: 'BCC signed emails' blind-copies completed Adobe Sign / DocuSign / EchoSign notifications sent to a list of named executives to █████@█████.com The intent (a central archive of executed agreements) is legitimate; the rule is undocumented, contains a typo in its name, lists recipients on the retired █████.com domain and one on █████.com (the previous tenant), and copies into a mailbox with no retention policy or hold.

A transport rule doing records-management work is fragile and hard to defend in audit. The 'Domain change disclaimer' rule (█████.com → █████.com) expired 31 Aug 2025 and is disabled — it can be removed.

Impact. Silent copying of contract documents with unclear ownership; possible failure as addresses change.

Recommendation. Document the rule's purpose and owner; update the recipient list to current █████.com addresses; apply a retention label/hold to the signed_documents mailbox; longer term, replace with a SharePoint records library fed by the e-signature integration. Delete the expired disclaimer rule and review 'block █████.org' for continued relevance.

Evidence: V4-TransportRules.json

5.3 Endpoint Security

C-5 · No Attack Surface Reduction policy exists — all 19 ASR rules unconfigured

CRITICAL	Effort S · Phase 0 · Verified (portal + Graph, 3 Sep 2026)	Microsoft security baseline
-----------------	--	-----------------------------

Observation. Zero ASR policies in Intune. All 19 rules score 0/9 and occupy ranks 1–19 in Secure Score (~14 percentage points behind a single policy).

The unconfigured rules are the controls that block LSASS credential theft, Office child-process execution, executable content from email, obfuscated scripts, WMI persistence, PSEXEC/WMI lateral movement, vulnerable signed drivers and ransomware behaviour. These map directly onto the initial-access, execution, credential-access and lateral-movement stages of a commodity ransomware intrusion. Combined with universal local-admin rights and no LAPS (H-6), a single phished user can become an estate-wide compromise.

Impact. Defender will see an intrusion; very little is configured to stop one.

Recommendation. Create one Intune ASR policy for all Windows devices: deploy all rules in Audit for 7–14 days, review the ASR report, then switch to Block (Warn where user impact is expected). Exclude only documented line-of-business paths. This is the highest return-on-effort item in the assessment.

Evidence: raw/11-intune-endpoint.json; raw/03-secure-score-actions.csv

H-4 · Device compliance is not a condition of access; the only compliance policy targets deprecated Android device-administrator

HIGH	Effort M · Phase 1 · Verified (Graph, 3 Sep 2026)	CIS 5.2.2.x
-------------	---	-------------

Observation. Verified: one compliance policy exists (Android device administrator, last modified 28 Mar 2022 — a management channel Microsoft retired 31 Dec 2024). No Windows compliance policy exists for 21 Windows endpoints and no Conditional Access policy references device compliance.

Device health — encryption, patch level, AV state, firewall — is not a condition of accessing company data. A compromised or unmanaged machine reaches SharePoint and Exchange on the same terms as a healthy one. Intune Threat Defense connectors are active but not referenced by any compliance policy, so mobile threat signals are collected and ignored.

Impact. No enforcement point between an unhealthy device and company data.

Recommendation. Create Windows 10/11 compliance policy (BitLocker, Secure Boot, TPM, AV on, firewall on, Defender risk ≤ Medium, minimum OS build) and iOS/Android compliance policies; wire into Conditional Access 'require compliant device' for Business Premium/E5 users; remove the dead Android device-administrator policy.

Evidence: V9-CompliancePolicies.json; raw/11-intune-endpoint.json

H-5 · No antivirus, BitLocker, firewall or security-baseline policy in Intune; 17 controls have regressed

HIGH	Effort M · Phase 1 · Verified (Graph + portal)	Microsoft security baseline
-------------	--	-----------------------------

Observation. Verified: zero endpoint security policies for AV, disk encryption and firewall; zero security baselines deployed (template intentCount = 0). Secure Score shows 17 previously-satisfied controls regressed —

real-time protection, cloud-delivered protection, firewall profiles, tamper protection, BitLocker, Credential Guard, built-in Administrator account.

Endpoint security is running on Windows and Defender defaults, and those defaults are decaying: 4 devices pending AV update, 3 with an inactive agent, 1 with the firewall off. Nothing is marked Planned or Risk-accepted in Secure Score, so the 114-item backlog is untriaged and configuration drift is invisible.

Impact. Protections that were once on are silently turning off; no key escrow for BitLocker recovery.

Recommendation. Deploy the Microsoft Security Baseline for Windows and the Defender for Endpoint baseline; create Intune AV policy (tamper protection, cloud protection High, real-time on), BitLocker policy with key escrow to Entra, and firewall policy (all profiles on). Triage Secure Score monthly and mark accepted risks.

Evidence: V9-BaselineTemplates.json; raw/11-intune-endpoint.json; raw/03-secure-score-actions.csv

H-6 · Every user is a local administrator; LAPS disabled; Global Admins are local admins on all Entra-joined devices

HIGH	Effort M · Phase 1 · Verified (Graph authorization policy + portal)	CIS 5.1.x; Microsoft baseline
-------------	---	-------------------------------

Observation. Registering users are added as local administrators, Global Administrators are added as local admins on every Entra-joined device, Entra LAPS is disabled and users can read their own BitLocker keys (AllowedToReadBitlockerKeysForOwnedDevice = true). Credential Guard is regressed and LSA protection unconfigured.

Universal local-admin rights, static unmanaged local-admin passwords, no LSASS credential-theft protection (C-5) and no Credential Guard is the standard chain by which a single phished user becomes estate-wide compromise. Adding GAs as local admins extends the blast radius of the highest-privilege accounts to every endpoint.

Impact. Trivial privilege escalation and lateral movement after any single endpoint compromise.

Recommendation. Enable Entra LAPS and deploy the Intune LAPS policy (rotate every 30 days / after use); set 'registering user added as local admin' to None and remove Global Administrators from device local-admin membership; deploy Endpoint Privilege Management or an account-protection policy to strip standing local admin; enable Credential Guard and LSA protection via the baseline (H-5); disable user self-recovery of BitLocker keys.

Evidence: V5-AuthorizationPolicy.json; raw/12-entra-identity.json

M-2 · Only 21 endpoints are managed against 622 mailboxes; 17 of 21 are workgroup-joined

MEDIUM	Effort L · Phase 2 · Verified (portal)	—
---------------	--	---

Observation. Whatever comprises the remainder of the estate — personal devices, dispensary POS and back-office PCs, contractor laptops — is outside Intune and Defender visibility while unmanaged devices retain full SharePoint access (H-8). 17 of 21 managed devices are workgroup rather than Entra-joined, which limits device-based Conditional Access and Windows Hello for Business.

Business Premium and E5 include Intune for 195 users; the 21-device footprint indicates enrolment was never rolled out. 'Managed by' shows Unknown on all devices and 0 critical assets are classified.

Impact. The majority of devices touching company data are invisible and unpoliced.

Recommendation. Inventory devices per location; Entra-join and auto-enrol all corporate Windows devices (Autopilot for new purchases); enrol store devices via Windows Autopilot self-deploying or shared-device mode; use app protection policies (MAM) for personal phones; classify POS and back-office servers as critical assets in Defender.

Evidence: raw/05-defender-devices.json; raw/11-intune-endpoint.json

M-3 · 9 of 21 devices carry High exposure; 2 run unsupported Windows 10 22H2; 1 has stopped reporting

MEDIUM	Effort S · Phase 1 · Verified (portal)	—
--------	--	---

Observation. Nine devices have unpatched exploitable vulnerabilities. Two devices ([REDACTED], desktop-[REDACTED]) run Windows 10 22H2, unsupported since October 2025 and receiving no security updates. One device (desktop-[REDACTED]) has sent no telemetry since 22 August 2026.

No Windows Update ring or patch-compliance policy was observed in Intune.

Impact. Known-exploitable vulnerabilities on nearly half the managed fleet; two devices permanently unpatched.

Recommendation. Replace or upgrade the two Windows 10 devices (or purchase ESU as a stop-gap); create Intune Windows Update rings with a 7-day quality-update deadline; work the Defender Vulnerability Management remediation list; investigate the silent device.

Evidence: raw/05-defender-devices.json

5.4 Collaboration & Sharing

C-1 · Anonymous, never-expiring, edit-capable external sharing is the tenant default

CRITICAL	Effort S · Phase 0 · Verified (portal, 2 Sep 2026)	CIS 7.2.3, 7.2.7, 7.2.9
----------	--	-------------------------

Observation. SharePoint and OneDrive external sharing are set to Anyone. The default link is 'Anyone with the link' with Edit permission, no expiration, and folder links permit upload.

Any of ~560 users clicking Share produces, by default, an unauthenticated, permanent, editable link that can be forwarded to anyone and used from any device. Nobody has to make a mistake for data to leave the organisation; the permissive path is the default path, and the audit trail attributes activity to an anonymous link rather than a person. Unmanaged devices have full access (H-8) and no label, DLP or retention policy governs the content (C-6).

Impact. Uncontrolled data egress of patient, customer, financial, deal and HR data; no chokepoint; no attribution.

Recommendation. Set SharePoint and OneDrive external sharing to 'New and existing guests' (or 'Existing guests' for OneDrive). Set default link type to 'Specific people', default permission to View, Anyone-link expiration to 30 days and Anyone folder links to View only. Review sites that already hold anonymous links via the SharePoint sharing report and expire them.

Evidence: raw/09-sharepoint-onedrive.json

H-1 · Any user can invite any external address as a guest; 143 guests exist with no lifecycle

HIGH	Effort M · Phase 1 · Verified (Graph user export, 3 Sep 2026)	CIS 5.1.6.2, 5.1.6.3
-------------	---	----------------------

Observation. Guest invitation is open to 'Anyone in the organization, including guests' from 'Any domain'. Verified count is 143 guest accounts (the portal sample showed 71): 62 have never signed in and 50 more have not signed in for over 90 days.

Guest domains include outside counsel and accountants ([REDACTED].com, [REDACTED].com, [REDACTED].com, [REDACTED].com and others), industry counterparties ([REDACTED].com, [REDACTED].com, [REDACTED].com) and 27 gmail.com plus other consumer mailboxes. There is no approval workflow, domain allow-list, expiry or access review. Duplicate and typo entries exist ([REDACTED].com / [REDACTED].com). Given three open legal matters and counsel present as guests, this is a confidentiality question as well as a security one.

Impact. Unreviewed external identities — 112 of 143 inactive or never used — retain whatever access they were granted, indefinitely.

Recommendation. Restrict guest invitations to admins and designated users (or members only); add a collaboration domain allow-list for counsel, accountants and partners; remove the 62 never-signed-in guests and disable the 50 stale ones; enable Entra access reviews for guests (quarterly) — available with the 27 E5 (P2) licenses for the reviewers; require guests to sign in with MFA via cross-tenant access settings.

Evidence: X-AllUsers-SignInActivity.json; raw/12-entra-identity.json

H-2 · Teams federation is open to every external domain; anonymous meeting join and open presenter rights

HIGH	Effort S · Phase 1 · Verified (portal, 2 Sep 2026)	CIS 8.2.1, 8.5.1, 8.5.6
-------------	--	-------------------------

Observation. 'Allow all external domains' with guest access, private calling and video enabled; no allow-list or block-list. Secure Score flags anonymous meeting join (0/1) and unrestricted presenters (0/2).

Any external Teams user can discover, chat with and call staff — the delivery path for the current wave of Teams-based phishing and fake-helpdesk social engineering. Anonymous join combined with anyone-can-present is a live meeting-hijack path.

Impact. External social-engineering and malware delivery channel outside email protections.

Recommendation. Switch external access to an allow-list of known partner domains; block Teams consumer (Skype) federation; set meeting policy so anonymous users wait in the lobby and only organizers/presenters can present; enable Defender for Office 365 protection for Teams (available on Business Premium/E5).

Evidence: raw/10-teams.json

H-8 · Unmanaged devices have full access to SharePoint and OneDrive; no idle-session timeout

HIGH	Effort S · Phase 1 · Verified (portal)	CIS 7.2.x, 1.3.x
-------------	--	------------------

Observation. Unmanaged device access = 'Allow full access from desktop apps, mobile apps and the web'; SharePoint idle session sign-out and Microsoft 365 idle session timeout are both off.

Combined with C-1, H-1 and M-2 (only 21 devices managed), personal and shop-floor devices reach company data freely and sessions on shared or kiosk machines never end.

Impact. Data lands on uncontrolled devices; shared-terminal sessions persist indefinitely.

Recommendation. Set unmanaged device access to 'Allow limited, web-only access' (this auto-creates the required CA policies); enable idle session sign-out at 1 hour with a 5-minute warning; enable Microsoft 365 idle session timeout.

Evidence: raw/09-sharepoint-onedrive.json; raw/15-m365-admin-org-settings.json

M-1 · Anonymous calendar sharing exposes meeting subjects and locations

MEDIUM	Effort S · Phase 1 · Verified (Exchange PowerShell)	CIS 1.3.3
--------	---	-----------

Observation. Verified: the Default Sharing Policy grants 'Anonymous:CalendarSharingFreeBusyReviewer' — detail-level free/busy (subjects, locations) to unauthenticated users. Secure Score 0/5.

Meeting subjects and attendee patterns of an acquisitive investment entity are commercially sensitive and are excellent reconnaissance for social engineering.

Impact. Information disclosure to anonymous parties.

Recommendation. Remove the Anonymous entry from the default sharing policy (retain *:CalendarSharingFreeBusySimple for federated partners); publish calendars only by explicit, authenticated invitation.

Evidence: X-SharingPolicies.json

5.5 Data Protection & Compliance

C-6 · No data protection framework: zero sensitivity labels, zero retention policies, no custom DLP

CRITICAL	Effort L · Phase 2 · Verified (portal 2 Sep + Security & Compliance PowerShell 3 Sep 2026)	CIS 3.1.1, 3.2.1, 3.3.1
----------	--	-------------------------

Observation. 0 sensitivity labels, 0 retention labels, 0 retention policies; only two Microsoft-default DLP policies (one in simulation). Purview is licensed for 195 users and essentially unconfigured.

Nothing classifies, encrypts, retains or prevents the loss of regulated data: patient and customer PII from dispensary operations, payment card data from retail, investor and deal documents from the investment entity, state-regulated compliance records, HR and payroll data. There is no defensible deletion schedule anywhere — Exchange, SharePoint, OneDrive, Teams — so data accumulates indefinitely, expanding the blast radius of any breach and the cost of any discovery request. Only 6 of 622 mailboxes have an online archive. Endpoint DLP is not onboarded. The Purview 'Information Protection 100% labeled' tile conflicts with the zero-label state and should be disregarded.

Impact. Regulatory exposure (state cannabis record-keeping, HIPAA where patient data is handled, PCI DSS), uncontrolled data growth, no encryption of sensitive content, and higher breach and litigation cost.

Recommendation. Phase 2: publish Purview's recommended label set (Public / General / Confidential / Highly Confidential) with a default label; create DLP policies for PCI (card numbers), US PII/PHI, and financial data with policy tips first, then block; create baseline retention policies (Exchange/OneDrive/SharePoint/Teams) aligned with state record-keeping periods confirmed by counsel; enable online archiving for user mailboxes; onboard Windows devices to Endpoint DLP. Instantiate a Compliance Manager assessment (e.g., NIST CSF / PCI DSS) to track progress.

Evidence: raw/08-purview-compliance.json; X-Mailboxes-HoldAuditArchive.json; JB-IPPS/*.json

C-7 · Three eDiscovery cases are open but zero mailboxes are under any hold

CRITICAL	Effort S · Phase 0 · Verified (Exchange + Security & Compliance PowerShell, 3 Sep 2026); Premium-case site holds unconfirmed	—
----------	--	---

Observation. Verified from the mailbox export: 0 of 622 mailboxes have litigation hold or any in-place/eDiscovery hold, while three eDiscovery cases exist — including '██████████' — '██████████' (created 29 Jul 2026), which names a digital-forensics vendor and suggests active or anticipated litigation.

With no retention policy (C-6) and no holds, preservation of relevant email depends entirely on users not deleting it. Deleted items age out of recoverable-items on default timers. A second case ('Confidential folder ██████████ OneDrive') has been open for over 14 months. Security & Compliance PowerShell confirms zero retention policies and zero hold policies on the Standard case; the two Premium cases were not enumerated by the cmdlet, so any site-level holds inside them should be confirmed with counsel — but no mailbox anywhere is held.

Impact. Spoliation risk in live legal matters; sanctions exposure; inability to demonstrate defensible preservation.

Recommendation. This week: confirm with outside counsel which custodians and date ranges require preservation, then apply eDiscovery holds (or litigation hold on the custodian mailboxes) within the existing cases, including SharePoint/OneDrive locations. Document the hold notice process. Then close or archive stale cases.

Evidence: X-Mailboxes-HoldAuditArchive.json; raw/08-purview-compliance.json

M-7 · Online archiving is enabled on 6 of 622 mailboxes; audit log is never proactively reviewed; audit retention unverified

MEDIUM	Effort S · Phase 2 · Verified (Exchange + Security & Compliance PowerShell, 3 Sep 2026)	CIS 3.1.1, 6.1.x
--------	---	------------------

Observation. Only 6 mailboxes have an active online archive. Unified audit logging is enabled and mailbox auditing is enabled on all 622 mailboxes (both positives), but there are no saved searches, no alert policies beyond defaults, and no custom audit-retention policy exists, so the default 180-day window applies (1 year for the 27 E5 users).

Without archives, mailboxes grow without bound and there is no lifecycle for leaver content. Audit retention on Business Premium is 180 days by default; E5 (27 seats) allows up to 1 year (10 years with add-on). State record-keeping obligations may exceed this.

Impact. Investigations older than the retention window are impossible; leaver mail has no home.

Recommendation. Enable online archiving for all user mailboxes with a default 2-year move-to-archive policy; create alert policies for suspicious forwarding, mass download, eDiscovery activity and admin role changes; verify audit retention and extend to 1 year for E5 users; schedule a monthly review of the Defender and Purview alert queues.

Evidence: X-Mailboxes-HoldAuditArchive.json; raw/08-purview-compliance.json

L-1 · Customer Lockbox is not enabled

LOW	Effort S · Phase 2 · Verified (Exchange PowerShell)	CIS 1.3.6
------------	---	-----------

Observation. Verified: CustomerLockboxEnabled = false. Microsoft support engineers can be granted access to content during a support case without explicit organisational approval. Lockbox is included in the 27 E5 licenses.

Impact. Third-party (Microsoft) access to regulated content is not gated on approval.

Recommendation. Enable Customer Lockbox in the Microsoft 365 admin center (Org settings → Security & privacy).

Evidence: X-OrgConfig.json

5.6 Tenant Hygiene**L-2 · Migration residue and tenant metadata gaps: legacy domains, foreign-tenant DNS records, unverified domain, missing privacy contact**

LOW	Effort S · Phase 1 · Verified (Graph + DNS)	—
------------	---	---

Observation. The primary domain moved from [REDACTED].com to [REDACTED].com; 25 accounts and several mail-flow rules still reference the old domain. [REDACTED].com DKIM CNAMEs and a transport rule reference the previous tenant ([REDACTED]). [REDACTED].com is added but unverified. Global privacy contact and privacy statement URL are unset. Several guest entries are typos or duplicates ([REDACTED].com / [REDACTED].com; [REDACTED].gmail.co).

With further acquisitions and tenant-to-tenant migrations planned, each migration will add similar residue unless a post-migration checklist is adopted (Section 8).

Impact. Misdelivery, confusion, and phishing lures that exploit near-identical domains.

Recommendation. Complete the [REDACTED].com → [REDACTED].com cut-over; remove foreign-tenant DNS records; verify or remove [REDACTED].com; set the privacy contact and statement URL; clean guest typos; adopt the acquisition onboarding baseline in Section 8.

Evidence: V10-Domains.json; dns_verification.csv; V4-TransportRules.json

L-3 · Licensing housekeeping: duplicate disabled subscriptions, 35 unassigned seats, failed migration batch, mail loop

LOW	Effort S · Phase 1 · Verified (portal)	—
------------	--	---

Observation. A disabled Business Basic subscription (171 seats, expiring 9 Sep 2026) duplicates an active one; a Power BI Premium PU subscription expired 19 Aug 2026; 35 licenses are purchased but unassigned while ~190 are assigned to dormant accounts. Exchange shows a 'possible mail loop' insight and a failed migration batch ('batch8').

Impact. Cost leakage and unresolved mail-flow errors.

Recommendation. Confirm the disabled Business Basic subscription is a renewal artefact before 9 Sep 2026; reclaim licenses from dormant accounts (H-11); resolve the mail loop and clean up the failed migration batch.

Evidence: raw/13-licenses-subscriptions.json; raw/07-exchange-online.json

6. What Is Working

The tenant is not neglected. The following controls are correctly configured and deserve explicit credit; several of them (the preset security policy, tenant-wide MFA and legacy-auth policies, complete Defender onboarding, mailbox auditing) are the foundations the roadmap builds on rather than replaces.

Control	Note
Standard preset security policy is On for all recipients with no exclusions	The strongest single element of the email posture; impersonation and mailbox-intelligence controls inside the preset score full marks.
Conditional Access 'MFA' and 'Block legacy authentication' policies are tenant-wide	Verified: both include All users and All applications with minimal exclusions.
Administrative MFA is fully covered	Secure Score 10/10 for MFA on administrative roles; Global Administrator count (3) is within Microsoft's recommended 2–4.
Mailbox auditing is enabled on all 622 mailboxes and unified audit logging is functional	Verified via Exchange PowerShell; the Secure Score item on mailbox auditing reflects an org-level default rather than per-mailbox state.
SPF is published with hard-fail on 33 of 35 domains	Verified by external DNS; only [REDACTED].org lacks SPF.
Defender for Endpoint onboarding is complete	21 of 21 devices onboarded, 0 with active malware; the EDR profile that does this is correct.
Zero external auto-forwards in the prior 7 days and all 33 mailbox forwards are internal	Good hygiene, pending the policy block in H-9.
Legacy authentication is blocked at both the Conditional Access and SharePoint layers	—
Password expiration is set to never expire	Matches current Microsoft and NIST guidance; Secure Score 8/8.
Admin consent workflow is enabled	Designated reviewer, notifications and 30-day expiry.
A Tenant Allow/Block List is actively maintained	An impersonation attempt was blocked in the week before assessment.
eDiscovery is in use and the 'Block htm attachments' transport rule is a sound control	—

7. Licensing: The Structural Constraint and Recommendation

The verified service-plan data settles a question the portal alone could not: Business Basic and Business Standard licences carry no Entra ID P1, Intune or Defender for Office 365 service plan. That has three consequences for this report.

1. Conditional Access is not licensed for ~365 users. The tenant-wide "MFA" policy technically evaluates them, but Microsoft's licensing terms require every user who benefits from a Conditional Access policy to hold Entra ID P1. The organisation is both under-protected and out of compliance with its licence terms.
2. Intune, Defender for Business/Endpoint, Defender for Office 365 (Safe Links, Safe Attachments, impersonation protection beyond the preset), Purview Information Protection and Endpoint DLP cannot be extended to those users at all.
3. The 21-device management footprint against 622 mailboxes, the 174 MFA-incapable identities and the absence of device-based access control are the visible symptoms.

7.1 Options

Option	What it unlocks	Considerations
A. Uplift Business Basic/Standard users to Business Premium (recommended)	Entra ID P1, Intune, Defender for Business, Defender for Office 365 P1, Purview Information Protection, Exchange archiving — one SKU, one policy set for everyone.	Highest per-seat cost but simplest to operate and the model Microsoft designs its SMB security baseline around. Reclaiming ~190 dormant seats (H-11) and the 35 unassigned seats offsets a meaningful share of the uplift.
B. Add Entra ID P1 (and optionally Defender for Business) to existing SKUs	Conditional Access and MFA governance for all users; endpoint protection if Defender for Business is added.	Lower cost; leaves Intune, Safe Links/Attachments and Purview gaps for those users; two policy tiers to maintain.
C. Tiered model — Business Premium for office/management staff, Business Basic + Entra P1 for store staff	Covers the highest-value identities fully; brings all users under Conditional Access.	Requires clear role-based licence groups and a joiner/leaver process; store devices still need a management answer (shared-device Intune or kiosk).

Recommendation

Adopt Option A, or Option C as a minimum, within 30 days. Sequence it with H-11 (dormant-account clean-up) so reclaimed seats fund the uplift, and license by group (dynamic groups by department/location) so future acquisitions inherit the correct entitlement automatically. The Phase 1 controls in this report are designed to be deployed to the Business Premium/E5 population first and extended to the remainder as licences land.

The 27 E5 licences already include Entra ID P2 (Privileged Identity Management, Identity Protection risk policies, access reviews), Defender for Identity, Customer Lockbox, Insider Risk and Communication Compliance. Several recommendations in this report (H-12, C-8, H-1, M-5, L-1) use those entitlements as they stand.

8. Acquisition Onboarding Security Baseline

the Client is actively acquiring businesses and locations; one tenant-to-tenant migration has been completed and one or two more are in planning. Several findings in this report are migration residue — DKIM records pointing at a previous tenant, mail-flow rules referencing retired domains and addresses, duplicate guests, unverified domains, dormant accounts. Without a standard, each migration adds to the backlog. IT Partner LLC recommends the following day-one baseline for every acquired tenant, domain and location, to be applied as part of the migration project rather than after it.

Area	Day-one baseline
Before migration	Run this same assessment on the acquired tenant; inventory domains, admins, guests, forwarding rules, OAuth grants and devices; identify regulated data (patient, card, financial) and any legal holds that must survive the move.
Domains	Verify each domain in the target tenant; publish SPF (-all), enable DKIM, publish DMARC (p=none with rua, then enforce); remove source-tenant DNS records; decide live vs parked and set parked domains to p=reject with a null MX.
Identity	Migrate users into licence groups that carry Business Premium; enforce MFA registration with Temporary Access Pass on day one; no standing admin roles — use PIM; disable source-tenant accounts and guests on cut-over; run the inactive-account report 30 days after.
Devices	Entra-join and Intune-enrol acquired Windows devices (Autopilot reset where practical); apply the compliance, ASR, AV, BitLocker, firewall and LAPS policy set; replace unsupported OS versions before they touch company data.
Collaboration	Migrated sites and OneDrives inherit the tenant sharing defaults (specific people, view, expiry); guests from the acquired business are re-invited under the domain allow-list and put on access review.
Data & compliance	Apply the default sensitivity label and baseline retention policies to migrated content; re-establish any legal holds in the target tenant before the source is decommissioned; confirm audit retention covers the state record-keeping period.
Mail flow	Recreate only documented transport rules; block external auto-forwarding; add executives from the acquired business to impersonation protection and Priority accounts.
Close-out	30-day post-migration review against this checklist; decommission the source tenant only after holds, archives and DNS are confirmed in the target.

9. Remediation Roadmap

The roadmap sequences every finding into four phases. Effort is sized S (under a day), M (one to five days) or L (a project of two or more weeks). Phase 0 requires no licence change and can begin immediately.

Phase 0 — Stabilise (Weeks 1–2)

Close the gaps an attacker would use this month, at near-zero cost.

ID	Severity	Action	Effort
C-8	Critical	A Global Administrator is flagged at risk (medium) and 15 other risky users are unremediated	S
C-3	Critical	Every strong MFA method is disabled in the Authentication methods policy; only Email OTP is enabled	S
C-7	Critical	Three eDiscovery cases are open but zero mailboxes are under any hold	S
C-2	Critical	DKIM is disabled on 34 of 35 domains and DMARC is absent on 21; every brand domain is spoofable	M
C-1	Critical	Anonymous, never-expiring, edit-capable external sharing is the tenant default	S
H-9	High	External auto-forwarding is not blocked by policy	S
H-13	High	A transport rule sets SCL –1 for any sender claiming a █████.com domain — a spoofable filtering bypass	S
H-7	High	Impersonation protection covers 1 user and 0 of 35 domains, with impersonation attempts already observed	S
C-5	Critical	No Attack Surface Reduction policy exists — all 19 ASR rules unconfigured	S

Phase 1 — Harden (Days 15–60)

Decide licensing, then make identity, device and collaboration controls enforceable.

ID	Severity	Action	Effort
—	Enabler	Licensing decision: Uplift Business Basic/Standard users to Business Premium (or add Entra ID P1 + Defender for Business) so Conditional Access, Intune and Defender for Office 365 can be applied tenant-wide. See Section 7.	M
C-4	Critical	174 of 717 identities (24%) cannot perform MFA; 365 users have no Conditional Access entitlement	M
H-12	High	No emergency-access (break-glass) account; all 24 privileged role assignments are permanent; PIM unused despite P2 entitlement	M
H-3	High	Admin-portal MFA and phishing-resistant admin MFA policies are Report-only; the risky sign-in policy covers one group	M
H-11	High	190 enabled accounts have not signed in for 90+ days (87 never); each is a licensed, MFA-less attack surface	M
H-1	High	Any user can invite any external address as a guest; 143 guests exist with no lifecycle	M

ID	Severity	Action	Effort
H-2	High	Teams federation is open to every external domain; anonymous meeting join and open presenter rights	S
H-4	High	Device compliance is not a condition of access; the only compliance policy targets deprecated Android device-administrator	M
H-5	High	No antivirus, BitLocker, firewall or security-baseline policy in Intune; 17 controls have regressed	M
H-6	High	Every user is a local administrator; LAPS disabled; Global Admins are local admins on all Entra-joined devices	M
H-8	High	Unmanaged devices have full access to SharePoint and OneDrive; no idle-session timeout	S
H-10	High	Standard users can register applications, create tenants and read their own BitLocker keys; user consent runs on a custom policy	S
M-1	Medium	Anonymous calendar sharing exposes meeting subjects and locations	S
M-3	Medium	9 of 21 devices carry High exposure; 2 run unsupported Windows 10 22H2; 1 has stopped reporting	S
M-4	Medium	E-signature BCC rule is undocumented and references legacy-tenant addresses	S
M-5	Medium	On-premises password protection is in Audit mode; no custom banned-password list; on-premises AD is unassessed	S
M-6	Medium	46 OAuth permission grants (33 tenant-wide) including mail, files and full site control are not inventoried	S
M-8	Medium	Device registration is unrestricted: any user may join up to 50 devices with no MFA required	S
L-2	Low	Migration residue and tenant metadata gaps: legacy domains, foreign-tenant DNS records, unverified domain, missing privacy contact	S
L-3	Low	Licensing housekeeping: duplicate disabled subscriptions, 35 unassigned seats, failed migration batch, mail loop	S

Phase 2 — Govern (Days 60–120)

Build the data-protection and compliance layer a regulated multi-state operator needs.

ID	Severity	Action	Effort
C-6	Critical	No data protection framework: zero sensitivity labels, zero retention policies, no custom DLP	L
M-2	Medium	Only 21 endpoints are managed against 622 mailboxes; 17 of 21 are workgroup-joined	L
M-7	Medium	Online archiving is enabled on 6 of 622 mailboxes; audit log is never proactively reviewed; audit retention unverified	S
L-1	Low	Customer Lockbox is not enabled	S
—	Enabler	On-premises AD assessment: Separate engagement: domain-controller hardening, LDAP signing/NTLM, Defender for Identity sensors (E5).	M

Phase 3 — Sustain (Ongoing)

Keep the posture from decaying and make every acquisition land securely.

ID	Severity	Action	Effort
—	Enabler	Acquisition onboarding security baseline: Day-one checklist for every acquired tenant, domain and location (Section 8).	M
—	Enabler	Operating rhythm: Monthly Secure Score triage, quarterly access reviews, alert-queue review, inactive-account report, DMARC report review.	S

Success measures

Measure	Today	Target (day 120)
Microsoft Secure Score	52.7%	≥ 75%
Identities unable to perform MFA	174	0 (all enabled accounts registered with Authenticator or passkey)
Domains with DKIM enabled / DMARC enforced	1 / 7	35 / 35
Users at risk unremediated	16	0, with automated risk policies
Privileged roles under PIM	0 of 24	24 of 24 + 2 break-glass accounts
Managed endpoints	21	All corporate Windows devices; store devices in shared-device mode
Enabled accounts inactive 90+ days	190	< 10, with monthly report
Guests without review	143	0 — quarterly access review
Retention policies / sensitivity labels / DLP policies	0 / 0 / 0 custom	Baseline set live in all workloads
Mailboxes under hold in open matters	0	All custodians, confirmed with counsel

Appendix A. Findings Register

ID	Sev.	Domain	Finding	Effort	Phase
C-1	Critical	Collaboration & Sharing	Anonymous, never-expiring, edit-capable external sharing is the tenant default	S	0
C-2	Critical	Email Security	DKIM is disabled on 34 of 35 domains and DMARC is absent on 21; every brand domain is spoofable	M	0
C-3	Critical	Identity & Access	Every strong MFA method is disabled in the Authentication methods policy; only Email OTP is enabled	S	0
C-4	Critical	Identity & Access	174 of 717 identities (24%) cannot perform MFA; 365 users have no Conditional Access entitlement	M	1
C-5	Critical	Endpoint Security	No Attack Surface Reduction policy exists — all 19 ASR rules unconfigured	S	0
C-6	Critical	Data Protection & Compliance	No data protection framework: zero sensitivity labels, zero retention policies, no custom DLP	L	2
C-7	Critical	Data Protection & Compliance	Three eDiscovery cases are open but zero mailboxes are under any hold	S	0
C-8	Critical	Identity & Access	A Global Administrator is flagged at risk (medium) and 15 other risky users are unremediated	S	0
H-1	High	Collaboration & Sharing	Any user can invite any external address as a guest; 143 guests exist with no lifecycle	M	1
H-2	High	Collaboration & Sharing	Teams federation is open to every external domain; anonymous meeting join and open presenter rights	S	1
H-3	High	Identity & Access	Admin-portal MFA and phishing-resistant admin MFA policies are Report-only; the risky sign-in policy covers one group	M	1
H-4	High	Endpoint Security	Device compliance is not a condition of access; the only compliance policy targets deprecated Android device-administrator	M	1
H-5	High	Endpoint Security	No antivirus, BitLocker, firewall or security-baseline policy in Intune; 17 controls have regressed	M	1
H-6	High	Endpoint Security	Every user is a local administrator; LAPS disabled; Global Admins are local admins on all Entra-joined devices	M	1
H-7	High	Email Security	Impersonation protection covers 1 user and 0 of 35 domains, with impersonation attempts already observed	S	0
H-8	High	Collaboration & Sharing	Unmanaged devices have full access to SharePoint and OneDrive; no idle-session timeout	S	1
H-9	High	Email Security	External auto-forwarding is not blocked by policy	S	0
H-10	High	Identity & Access	Standard users can register applications, create tenants and read their own BitLocker keys; user consent runs on a custom policy	S	1

ID	Sev.	Domain	Finding	Effort	Phase
H-11	High	Identity & Access	190 enabled accounts have not signed in for 90+ days (87 never); each is a licensed, MFA-less attack surface	M	1
H-12	High	Identity & Access	No emergency-access (break-glass) account; all 24 privileged role assignments are permanent; PIM unused despite P2 entitlement	M	1
H-13	High	Email Security	A transport rule sets SCL -1 for any sender claiming a [REDACTED].com domain — a spoofable filtering bypass	S	0
M-1	Medium	Collaboration & Sharing	Anonymous calendar sharing exposes meeting subjects and locations	S	1
M-2	Medium	Endpoint Security	Only 21 endpoints are managed against 622 mailboxes; 17 of 21 are workgroup-joined	L	2
M-3	Medium	Endpoint Security	9 of 21 devices carry High exposure; 2 run unsupported Windows 10 22H2; 1 has stopped reporting	S	1
M-4	Medium	Email Security	E-signature BCC rule is undocumented and references legacy-tenant addresses	S	1
M-5	Medium	Identity & Access	On-premises password protection is in Audit mode; no custom banned-password list; on-premises AD is unassessed	S	1
M-6	Medium	Identity & Access	46 OAuth permission grants (33 tenant-wide) including mail, files and full site control are not inventoried	S	1
M-7	Medium	Data Protection & Compliance	Online archiving is enabled on 6 of 622 mailboxes; audit log is never proactively reviewed; audit retention unverified	S	2
M-8	Medium	Identity & Access	Device registration is unrestricted: any user may join up to 50 devices with no MFA required	S	1
L-1	Low	Data Protection & Compliance	Customer Lockbox is not enabled	S	2
L-2	Low	Tenant Hygiene	Migration residue and tenant metadata gaps: legacy domains, foreign-tenant DNS records, unverified domain, missing privacy contact	S	1
L-3	Low	Tenant Hygiene	Licensing housekeeping: duplicate disabled subscriptions, 35 unassigned seats, failed migration batch, mail loop	S	1

Appendix B. Email Authentication by Domain (verified 3 Sep 2026)

MX records for all 35 domains point to Exchange Online. "Users" is the number of member accounts whose sign-in name uses the domain.

Domain	Users	SPF	DKIM	DMARC	Reporting	Note
████████.com	245	Hard fail (-all)	Disabled	No record	No	
████████-ma.com	130	Hard fail (-all)	Disabled	No record	No	
████████.org	65	None	Enabled	p=none	No	No SPF record
████████-mi.com	50	Hard fail (-all)	Disabled	No record	No	
████████.co	38	Hard fail (-all)	Disabled	No record	No	
████████.com	25	Hard fail (-all)	Disabled	No record	No	
████████.com	24	Hard fail (-all)	Disabled	No record	No	
████████.co	21	Hard fail (-all)	Disabled	No record	No	
████████.com	12	Hard fail (-all)	Disabled	No record	No	
████████.onmicrosoft.com	7	Hard fail (-all)	Disabled	No record	No	
████████.com	6	Hard fail (-all)	Disabled	No record	No	
████████.co	6	Soft fail (~all)	Disabled	p=quarantine	Yes	
████████.co	6	Hard fail (-all)	Disabled	No record	No	
████████.shop	5	Hard fail (-all)	Disabled	p=none	No	
████████.org	4	Soft fail (~all)	Disabled	p=none	No	
████████.com	1	Hard fail (-all)	Disabled	p=reject	Yes	
████████.org	1	Hard fail (-all)	Disabled	p=none	No	
████████.com	1	Hard fail (-all)	Disabled	p=none	No	
████████.com	1	Soft fail (~all)	Disabled	p=quarantine	No	DKIM CNAMEs point to foreign tenant (████████)
████████.co	1	Hard fail (-all)	Disabled	p=quarantine	Yes	
████████.com	0	Hard fail (-all)	Disabled	p=quarantine	Yes	
████████.com	0	Hard fail (-all)	Disabled	No record	No	
████████-al.com	0	Hard fail (-all)	Disabled	No record	No	

Domain	Users	SPF	DKIM	DMARC	Reporting	Note
██████████-az.com	0	Hard fail (-all)	Disabled	No record	No	
██████████-ca.com	0	Hard fail (-all)	Disabled	No record	No	
██████████-ct.com	0	Hard fail (-all)	Disabled	No record	No	
██████████-fl.com	0	Hard fail (-all)	Disabled	No record	No	
██████████-ga.com	0	Hard fail (-all)	Disabled	No record	No	
██████████-nj.com	0	Hard fail (-all)	Disabled	No record	No	
██████████-ny.com	0	Hard fail (-all)	Disabled	No record	No	
██████████-va.com	0	Hard fail (-all)	Disabled	No record	No	
██████████.com	0	Hard fail (-all)	Disabled	p=reject	Yes	
██████████.co	0	Hard fail (-all)	Disabled	p=none	Yes	
██████████.co	0	Hard fail (-all)	Disabled	p=none	Yes	
██████████.com	0	Hard fail (-all)	Disabled	p=quarantine	Yes	

Appendix C. Conditional Access and Privileged Roles

C.1 Conditional Access policies (verified detail)

Policy	Author	State	Scope and controls	Assessment
MFA	Customer	On	All users, all apps; 3 excluded users; grant = MFA	Covers whole tenant. Exclusions need review (break-glass?)
Block legacy authentication	Customer	On	All users; client apps = Exchange ActiveSync + Other; 1 excluded user; grant = Block	Correctly scoped
Microsoft-managed: MFA for admins accessing Microsoft Admin Portals	Microsoft	Report-only	14 admin roles; Microsoft Admin Portals; grant = MFA	Not enforcing
Microsoft-managed: MFA and reauthentication for risky sign-ins	Microsoft	On	One group only; sign-in risk = High; grant = MFA; sign-in frequency every time	Scoped to a single group, High risk only
Baseline Security Mode: Require phishing-resistant MFA for admins	Microsoft baseline	Report-only	19 admin roles; all apps; 1 excluded user; auth strength = phishing-resistant	Not enforcing; created 20 Jul 2026

C.2 Directory role assignments (all permanent; no PIM eligibility)

Role	Holders	Members
Global Administrator	3	[REDACTED] [REDACTED], [REDACTED] [REDACTED] (IT Partner), [REDACTED] [REDACTED]
Exchange Administrator	3	[REDACTED] [REDACTED], [REDACTED] [REDACTED], [REDACTED] [REDACTED]
User Administrator	3	[REDACTED] [REDACTED], [REDACTED] [REDACTED], [REDACTED] [REDACTED]
SharePoint Administrator	2	[REDACTED] [REDACTED], [REDACTED] [REDACTED]
Teams Administrator	2	[REDACTED] [REDACTED], [REDACTED] [REDACTED]
Helpdesk Administrator	2	[REDACTED] [REDACTED], [REDACTED] [REDACTED]
Service Support Administrator	2	[REDACTED] [REDACTED], [REDACTED] [REDACTED]
Global Reader	2	[REDACTED] [REDACTED], [REDACTED] [REDACTED]
Purview Workload Content Writer	2	[REDACTED] [REDACTED], [REDACTED] [REDACTED]
AI Administrator	1	[REDACTED] [REDACTED]
User Experience Success Manager	1	[REDACTED] [REDACTED]

Appendix D. Verification Log and Scope Exclusions

D.1 Items flagged for verification after portal collection

#	Item	Outcome
V-1	Conditional Access scope, exclusions and controls	Verified 3 Sep 2026 (Graph). Findings C-4, H-3, H-12 updated.
V-2	Licensing entitlement for CA / Intune / Defender	Verified 3 Sep 2026 (SKU service plans). Structural finding confirmed.
V-3	SPF and DMARC for all 35 domains	Verified 3 Sep 2026 (external DNS). C-2 expanded; Appendix B.
V-4	Transport rule conditions and actions	Verified 3 Sep 2026. H-13 confirmed as bypass; M-4 downgraded to documentation issue.
V-5	User consent effective state	Partially verified: custom policy 'rm-consent-policy-v1' identified; contents not retrieved.
V-6	Break-glass and PIM	Verified 3 Sep 2026: no break-glass, no PIM eligibility, all assignments permanent (H-12).
V-7	Legal-hold status in eDiscovery cases	Verified 3 Sep 2026: 0 holds on all 622 mailboxes; the Standard case has no hold policy. The two Premium cases were not returned by Get-ComplianceCase (needs -CaseType AdvancedEDiscovery); site-level holds in those cases remain unconfirmed — C-7.
V-8	Audit log retention period	Verified 3 Sep 2026: no custom audit retention policy exists, so defaults apply (180 days; 1 year for E5-licensed users).
V-9	Intune security baselines	Verified 3 Sep 2026: zero baselines deployed (H-5).
V-10	Live vs parked domains	Inferred from user population: 14 domains carry users; 21 carry 0–1 users. Client to confirm parked list.

D.2 Not assessed

- On-premises Active Directory (domain controllers, GPOs, NTLM/LDAP posture) — separate engagement recommended
- SharePoint site-level sharing, anonymous-link inventory and 'more external sharing settings'
- Teams meeting/messaging/app-permission policy detail
- Intune enrolment restrictions, app protection (MAM) policies, Windows Update rings
- Shared-mailbox sign-in state (88 shared mailboxes)
- Insider Risk, Communication Compliance and Information Barriers policy detail
- Defender for Cloud Apps and app-governance configuration
- Point-of-sale, seed-to-sale and other line-of-business systems outside Microsoft 365

D.3 Evidence package

Portal captures (raw/01–15), the Secure Score action export, the Graph/Exchange/Security & Compliance PowerShell exports (V1–V10, X-*) and the DNS verification table are retained by IT Partner LLC and available to the client on request. Figures are point-in-time as at the dates stated.