AroraMSP

Microsoft 365 Consulting

Microsoft 365 Tenant Health Audit

Prepared for

Brightpath Logistics Inc.

Document reference	BPL-M365-AUDIT-2026-04
Prepared by	Himanshu Arora, AroraMSP
Date	April 2026
Version	1.0
Classification	Confidential
Distribution	Chief Operating Officer, IT Manager, Finance Director

Document Control

Client	Brightpath Logistics Inc.
Engagement	Microsoft 365 Tenant Health Audit
Document reference	BPL-M365-AUDIT-2026-04
Version	1.0
Prepared by	Himanshu Arora, AroraMSP
Date of issue	14 April 2026
Classification	Confidential
Distribution	Chief Operating Officer, IT Manager, Finance Director

Revision history

Version	Date	Author	Summary
0.1	10 April 2026	Himanshu Arora	Draft for internal review
1.0	14 April 2026	Himanshu Arora	Final release to client

Executive Summary

Engagement context

Brightpath Logistics Inc. commissioned AroraMSP to conduct an independent health audit of its Microsoft 365 tenant. The engagement ran over five business days and covered identity, access, email security, collaboration workloads, endpoint posture, and licensing. The objective was to provide the executive team with an evidence-based view of security posture and cost efficiency, together with a prioritized remediation roadmap suitable for a ninety-day execution window.

Overall posture

The tenant is operational and supports the business effectively at a functional level. However, the audit identified fifteen findings, several of which are high-severity security gaps that require immediate attention. Default Microsoft protections are in place, but the environment lacks the tenant-wide Conditional Access baseline, privileged access controls, and email authentication enforcement that Microsoft recommends for any production tenant in 2026. A number of these gaps are common in tenants that were set up several years ago and have not been reviewed against current best practice.

Findings at a glance

HIGH	MEDIUM	LOW
6 Immediate or 14-day action	8 30 to 60-day action	1 Housekeeping or 90-day

Top three priorities

1. **EML-02** Investigate external auto-forwarding on three mailboxes within forty-eight hours. Treat as suspected compromise pending review. Disable automatic external forwarding tenant-wide.

2. **IDA-03, IDA-04** Establish two break-glass accounts and implement tenant-wide Conditional Access for MFA enforcement. These controls together close the largest standing access-management gap.

3. **EML-01** Begin the ninety-day DMARC progression from p=none to p=reject. Start aggregate report collection immediately so enforcement can begin at day thirty.

Quantified cost saving

Licensing and shared-mailbox findings together represent an estimated **USD 8,064 per year** in recoverable cost once the eighteen reclaimable E3 licences and four shared-mailbox Business Basic assignments are resolved. This saving materially offsets the remediation effort required for the high-severity findings.

Scope and Methodology

In scope

• Tenant configuration review across Entra ID, Exchange Online, SharePoint Online, OneDrive, Teams, and Intune.

• Identity and access posture including Conditional Access, MFA coverage, privileged role assignments, break-glass account configuration, and Self-Service Password Reset.

• Hybrid identity review of Azure AD Connect deployment, agent version, synchronization health, and sync rule inventory.

• Email authentication review of SPF, DKIM, and DMARC records for the primary domain.

• Exchange Online configuration review of anti-phishing, anti-spam, connector configuration, forwarding rules, and mailbox audit settings.

• Collaboration workload settings covering Teams federation, guest access, external sharing on OneDrive and SharePoint, and Sensitivity Label deployment.

• Endpoint management review of Intune policies, compliance configuration, and Conditional Access device requirements.

• Licensing review identifying unused, over-allocated, or incorrectly assigned licences.

Out of scope

• Penetration testing, red-team exercises, or active exploitation of identified weaknesses.

• Microsoft 365 data backup, archive, or disaster recovery tooling.

• Third-party SaaS applications integrated with Entra ID beyond federation posture review.

• Network infrastructure, perimeter firewalls, and on-premises Active Directory forest health beyond AD Connect scope.

• Remediation execution. This document describes findings and recommendations only.

Methodology

Data collection was read-only and non-intrusive. No configuration changes were made to the tenant. The following sources were used:

• Microsoft Graph PowerShell SDK for tenant, user, role, and policy enumeration.

• Exchange Online PowerShell v3 for mailbox configuration, transport rules, and anti-spam policy review.

• Microsoft Entra admin centre for visual inspection of Conditional Access, Authentication Methods, and Identity Protection dashboards.

• Microsoft Secure Score and Compliance Manager baseline comparison.

• DNS resolution against authoritative records for SPF, DKIM, DMARC, and MX validation.

• Licensing centre and Microsoft 365 admin centre for licence usage and assignment inventory.

Engagement timeline

Day	Phase	Activities
Day 1	Kick-off and access	Engagement brief, delegated access provisioning, scope confirmation with stakeholders.

Day	Phase	Activities
Days 2-3	Data collection	Automated extraction and manual review of all in-scope configuration.
Day 4	Analysis	Severity assessment, correlation of findings, licence utilization modelling.
Day 5	Report and walkthrough	Draft delivery, executive walkthrough, final report issued.

Environment Overview

Tenant

Primary domain	brightpath-logistics.com
Secondary domain	bpl-freight.com (added post-acquisition, March 2025)
Tenant region	North America
Tenant creation	November 2021
Active users	85
Primary identity source	On-premises Active Directory via Azure AD Connect

Licensing summary

Licence SKU	Purchased	Assigned
Microsoft 365 Business Premium	72	72
Microsoft 365 E3	13	5 active, 8 unassigned
Exchange Online Plan 1 (shared mailbox allocations in error)	4	4
Microsoft Teams Phone	12	12
Power BI Pro	6	6

Findings Summary

The following table lists all fifteen findings in priority order. Severity is assigned on a three-level scale. Each finding is expanded with observation, risk, and recommendation detail in the next section.

ID	Category	Finding	Severity
IDA-01	Identity and Access	Legacy authentication not blocked at tenant level	HIGH
IDA-02	Identity and Access	Six accounts hold the Global Administrator role	HIGH
IDA-03	Identity and Access	No break-glass emergency access account configured	HIGH
IDA-04	Identity and Access	No Conditional Access policy enforcing tenant-wide MFA	HIGH
IDA-05	Identity and Access	AD Connect agent is outdated by two major releases	MEDIUM
IDA-06	Identity and Access	Self-Service Password Reset not enabled for standard users	MEDIUM
EML-01	Email Security	DMARC record published at policy p=none	HIGH
EML-02	Email Security	External auto-forwarding enabled on three mailboxes	HIGH
EML-03	Email Security	Mailbox audit logging disabled on seven mailboxes	MEDIUM
EML-04	Email Security	Eleven shared mailboxes have passwords set, four carry licences	MEDIUM
COL-01	Collaboration and Endpoint	Teams external access and guest access are unrestricted	MEDIUM
COL-02	Collaboration and Endpoint	Intune licences assigned but no device policies deployed	MEDIUM
COL-03	Collaboration and Endpoint	OneDrive retention and external sharing not configured	LOW
LIC-01	Licensing and Cost	Eighteen E3 licences recoverable	MEDIUM
LIC-02	Licensing and Cost	Fourteen inactive user accounts remain enabled	MEDIUM

Detailed Findings

Identity and Access

IDA-01 Legacy authentication not blocked at tenant level

Category	Severity	Effort	Priority
Identity and Access	HIGH	1 hour configuration plus 7-day monitoring window	Within 7 days

Observation

Basic Authentication flows remain permitted across the tenant. Security Defaults are disabled in favour of granular Conditional Access. However, no Conditional Access policy currently blocks legacy authentication protocols such as POP, IMAP, SMTP AUTH, or older Outlook clients using basic authentication.

Risk

Legacy authentication cannot enforce multi-factor authentication under any circumstance. Accounts using these protocols remain exposed to password spray and credential stuffing attacks. This is the most common entry vector observed in tenant compromises.

Recommendation

Create a Conditional Access policy named "Block Legacy Authentication" targeting all users and all cloud apps. Set Client apps to "Exchange ActiveSync clients" and "Other clients". Configure in report-only mode for seven days to confirm no legitimate workload depends on legacy authentication, then enforce.

IDA-02 Six accounts hold the Global Administrator role

Category	Severity	Effort	Priority
Identity and Access	HIGH	3 hours including role usage audit and reassignment	Within 14 days

Observation

Six accounts are currently assigned the Global Administrator role. Microsoft guidance recommends keeping standing Global Administrator count to no more than four, preferably two. There is no evidence of Privileged Identity Management eligibility or just-in-time elevation in use.

Risk

Each Global Administrator represents a maximum-value target. Excess assignments increase the blast radius of a single compromised credential. Standing privileged access without just-in-time elevation is inconsistent with least-privilege principles.

Recommendation

Reduce the standing Global Administrator count to two. Reassign the remaining four accounts to narrower roles such as Exchange Administrator, User Administrator, or Intune Administrator. Where licensing permits Entra ID P2, enable Privileged Identity Management for eligible elevation.

IDA-03 No break-glass emergency access account configured

Category	Severity	Effort	Priority
Identity and Access	HIGH	2 hours	Within 7 days

Observation

All administrative accounts are subject to Conditional Access policies and multi-factor authentication enforcement. No dedicated break-glass account exists excluded from Conditional Access. In the event of a misconfiguration, MFA provider outage, or identity federation failure, the tenant can become administratively inaccessible.

Risk

Administrative lockout can prevent recovery during an outage or active security incident. Microsoft published guidance recommends two break-glass accounts per tenant as standard practice.

Recommendation

Create two break-glass accounts on the tenant onmicrosoft.com domain. Assign the Global Administrator role to both. Exclude these accounts from every Conditional Access policy. Set 16-character randomly generated passwords stored in a sealed physical location. Configure sign-in log alerting for any authentication event on either account.

IDA-04 No Conditional Access policy enforcing tenant-wide MFA

Category	Severity	Effort	Priority
Identity and Access	HIGH	4 hours including testing and phased rollout	Within 14 days

Observation

Multi-factor authentication is configured per-user on some accounts but is not enforced tenant-wide via Conditional Access. Twenty-three accounts including four service accounts currently sign in without MFA. Per-user MFA is the legacy approach and does not integrate with sign-in risk or contextual conditions.

Risk

Inconsistent MFA coverage allows attackers to target users with MFA disabled. Per-user MFA does not respond to risky sign-in signals, unfamiliar locations, or unmanaged devices.

Recommendation

Create a Conditional Access policy named "Require MFA for all users" targeting all users and all cloud apps, with exclusions limited to break-glass accounts and the directory synchronization service principal. Apply Authentication Strengths to require phishing-resistant methods for administrative roles. Disable per-user MFA once the tenant-wide policy is verified.

IDA-05 AD Connect agent is outdated by two major releases

Category	Severity	Effort	Priority
Identity and Access	MEDIUM	4 hours including change window coordination	Within 30 days

Observation

The Azure AD Connect synchronization agent is at version 2.1.20.0, released in August 2022. The current supported release is version 2.4.x. Microsoft retires AD Connect versions older than eighteen months and stops synchronization from unsupported agents.

Risk

An unsupported agent can cease synchronizing identities without notice, breaking hybrid authentication for every user. Newer releases include security fixes and the LocalDB engine upgrade.

Recommendation

Schedule an in-place upgrade of AD Connect to the latest supported release during a maintenance window. Pre-upgrade: validate current sync rules, document any custom rules, back up the AdSyncTools directory, and verify connector configuration. Post-upgrade: confirm a full synchronization cycle completes successfully.

IDA-06 Self-Service Password Reset not enabled for standard users

Category	Severity	Effort	Priority
Identity and Access	MEDIUM	2 hours configuration plus user communication	Within 30 days

Observation

Self-Service Password Reset is enabled for administrator accounts only. Standard users must contact the IT help desk to reset passwords, increasing operational load and extending productivity loss during account lockouts.

Risk

SSPR registration also drives MFA registration coverage, because both processes share the same authentication methods. Leaving SSPR disabled leaves users without a recovery path during off-hours.

Recommendation

Enable SSPR for all users via the Entra admin center. Require registration through the Authentication Methods policy. Configure mobile phone, authenticator app, and security questions as registration methods. Communicate the rollout to users two weeks in advance.

Email Security and Exchange

EML-01 DMARC record published at policy p=none

Category	Severity	Effort	Priority
Email Security and Exchange	HIGH	2 hours to configure monitoring, plus 45 to 60 days progressive enforcement	Within 14 days

Observation

The DMARC TXT record at _dmarc.brightpath-logistics.com is configured with policy p=none. SPF passes for Microsoft 365 and DKIM is signed on both default selectors. However, DMARC at p=none instructs receiving mail servers to take no action on messages that fail authentication.

Risk

The Brightpath domain remains exploitable for external email spoofing. Attackers can send phishing or business email compromise messages that appear to originate from brightpath-logistics.com, and recipients mail servers will not reject them on DMARC grounds.

Recommendation

Deploy a DMARC aggregate-report processor to collect reports for thirty days. Confirm every legitimate sending source produces aligned messages. Transition progressively: p=quarantine pct=25, monitor fourteen days, p=quarantine pct=100, then p=reject.

EML-02 External auto-forwarding enabled on three mailboxes

Category	Severity	Effort	Priority
Email Security and Exchange	HIGH	2 hours investigation plus 1 hour policy configuration	Immediate, within 48 hours

Observation

Three user mailboxes have Outlook rules configured to automatically forward all incoming messages to external addresses. Forward targets include one Gmail address and two unverified third-party domains. The Outbound Spam Filter policy does not currently block automatic external forwarding.

Risk

External auto-forwarding is a recognized indicator of compromised mailboxes and data exfiltration. Attackers frequently create forwarding rules to silently exfiltrate correspondence following credential compromise.

Recommendation

Immediately review the three flagged rules with affected mailbox owners. If unauthorized, remove rules, force password reset, invalidate all active sessions, and review sign-in logs for ninety days. Configure the default Outbound Spam Filter policy to disable automatic external forwarding.

EML-03 Mailbox audit logging disabled on seven mailboxes

Category	Severity	Effort	Priority
Email Security and Exchange	MEDIUM	1 hour	Within 30 days

Observation

Exchange Online mailbox auditing is enabled by default at the tenant level. However, seven mailboxes have the AuditEnabled property set to False, likely inherited from a configuration that predates the January 2019 default-on change for mailbox auditing.

Risk

Incident response for mailbox access, delegated actions, and rule changes is not possible on audit-disabled mailboxes. If a compromise occurs, forensic evidence required to determine scope of access is unavailable.

Recommendation

Run Set-Mailbox -Identity -AuditEnabled $true against each of the seven mailboxes. Validate that the Unified Audit Log is enabled at the organisation level. Confirm AuditAdmin, AuditDelegate, and AuditOwner scopes include the recommended actions.

EML-04 Eleven shared mailboxes have passwords set, four carry licences

Category	Severity	Effort	Priority
Email Security and Exchange	MEDIUM	2 hours	Within 30 days

Observation

The tenant contains eleven shared mailboxes. All eleven have user account passwords set and are not blocked from interactive sign-in. Four have a Microsoft 365 Business Basic licence assigned, which is not required for shared mailboxes under fifty gigabytes.

Risk

Shared mailboxes with enabled sign-in function as interactive identities. They can be used for credential theft and are often excluded from MFA enforcement. Licensing shared mailboxes is also an unnecessary recurring cost.

Recommendation

Block sign-in on all eleven shared mailboxes using Set-User -BlockCredential $true. Remove the four Business Basic licences. Verify FullAccess and SendAs delegation permissions are correctly assigned to intended staff users.

Collaboration and Endpoint

COL-01 Teams external access and guest access are unrestricted

Category	Severity	Effort	Priority
Collaboration and Endpoint	MEDIUM	3 hours including partner-domain inventory and policy configuration	Within 30 days

Observation

Microsoft Teams is configured with default federation and guest-access settings. External access is open to all domains. Guest access is enabled and any user can create guest accounts. No Sensitivity Labels are applied to Teams or their underlying Microsoft 365 Groups.

Risk

Unrestricted federation allows unsolicited Teams contact from any domain, which has been used as a phishing vector. Unrestricted guest creation can result in data sprawl and unmonitored external collaboration.

Recommendation

Restrict external access to explicitly allowed domains in the Teams admin centre. Restrict guest creation to designated users through a Microsoft 365 Groups policy in Entra. Deploy Sensitivity Labels aligned to internal, confidential, and highly confidential classifications.

COL-02 Intune licences assigned but no device policies deployed

Category	Severity	Effort	Priority
Collaboration and Endpoint	MEDIUM	12 hours for baseline deployment across Windows and mobile	Within 60 days

Observation

Seventy-two Microsoft 365 Business Premium licences include Intune. No compliance policies, configuration profiles, or app protection policies are currently deployed. Devices access corporate email and files without any device-management or data-protection controls.

Risk

Unmanaged devices can access Exchange Online, SharePoint, and Teams. In the event of a lost device or departing employee, there is no mechanism to revoke access or wipe corporate data.

Recommendation

Deploy a baseline Intune configuration: compliance policy requiring encryption and PIN, app protection policy for Outlook mobile and Teams mobile, and a Conditional Access policy requiring compliant access to Exchange Online. Use Windows Autopilot for new device provisioning.

COL-03 OneDrive retention and external sharing not configured to business standards

Category	Severity	Effort	Priority
Collaboration and Endpoint	LOW	3 hours	Within 90 days

Observation

OneDrive retention is set to the default thirty days for deleted files. No retention policy is configured for compliance or legal-hold scenarios. Users can share OneDrive files externally by default with no restriction.

Risk

There is a gap in data retention for any regulated workload or future e-discovery requirement. External sharing permissions may not match Brightpath stated collaboration policy.

Recommendation

Align OneDrive and SharePoint external sharing settings with Brightpath written collaboration policy. Configure a Purview retention policy matching documented records management requirements. Review OneDrive external-sharing permissions and restrict anonymous link creation.

Licensing and Cost

LIC-01 Eighteen E3 licences recoverable

Category	Severity	Effort	Priority
Licensing and Cost	MEDIUM	3 hours	Within 30 days

Observation

The tenant holds thirteen Microsoft 365 E3 licences, of which eight are unassigned. Ten licences are assigned to accounts with no sign-in activity in the past sixty days. Five have been confirmed by HR as former employees. In total, eighteen E3 licences can be reclaimed.

Risk

At the published list price of approximately USD 36.00 per user per month, eighteen unused licences represent approximately USD 7,776 per year in wasted spend.

Recommendation

Disable the five confirmed former-employee accounts and revoke licences immediately. Remove licences from the ten inactive accounts pending manager confirmation. Return unassigned licences to the available pool and negotiate a licence reduction at the next renewal cycle.

LIC-02 Fourteen inactive user accounts remain enabled

Category	Severity	Effort	Priority
Licensing and Cost	MEDIUM	2 hours	Within 14 days

Observation

Fourteen user accounts have shown no sign-in activity in the past ninety days. Cross-referencing against HR records identifies five as former employees with termination dates from three to fourteen months ago. The remaining nine are inactive contractors or dormant accounts.

Risk

Dormant enabled accounts are a recognized attack vector. Credentials may be present in publicly leaked breach corpora, and the accounts are not subject to active MFA challenge through normal use.

Recommendation

Immediately disable the five former-employee accounts, move them to a designated "Former Employees" Entra group, and revoke active sessions. Convert the nine inactive contractor accounts to disabled state pending business confirmation. Implement a quarterly Entra Access Review.

Remediation Roadmap

The recommended execution window is ninety days. Activity is phased to front-load high-severity risk reduction while sequencing dependent work appropriately.

Days 0-7	Contain and stabilize
	• EML-02: Investigate three external forwarding rules, act on any compromise indicators, and disable tenant-wide automatic external forwarding.
	• IDA-03: Create two break-glass accounts, exclude them from all Conditional Access policies, and enable sign-in alerting.
	• IDA-01: Deploy Conditional Access policy blocking legacy authentication in report-only mode.

Days 8-14	Strengthen core access
	• IDA-04: Deploy Conditional Access policy requiring MFA for all users in report-only mode, then enforce.
	• IDA-02: Reduce standing Global Administrator count from six to two. Reassign remaining admins to narrower roles.
	• LIC-02: Disable fourteen inactive accounts and revoke sessions. Implement Entra Access Review.
	• EML-01: Deploy DMARC aggregate report processor and begin thirty-day monitoring at p=none.

Days 15-30	Tighten controls and recover cost
	• IDA-01: Enforce Conditional Access policy blocking legacy authentication after monitoring window.
	• IDA-05: Upgrade AD Connect to current supported release.
	• IDA-06: Enable Self-Service Password Reset for all users.
	• EML-03: Enable mailbox audit logging on the seven affected mailboxes.
	• EML-04: Block sign-in on eleven shared mailboxes and recover four licences.
	• LIC-01: Reclaim eighteen E3 licences.

Days 31-60	Collaboration and endpoint

	• COL-01: Restrict Teams external access to partner domains, deploy Sensitivity Labels, restrict guest creation.
	• COL-02: Deploy baseline Intune compliance, configuration, and app protection policies.
	• EML-01: Transition DMARC to p=quarantine pct=25 then pct=100.

Days 61-90	Governance and retention
	• COL-03: Configure OneDrive and SharePoint retention and external sharing to match business policy.
	• EML-01: Transition DMARC to p=reject.
	• Establish quarterly Entra Access Review, monthly Secure Score trending, and annual Conditional Access review.

Licensing Optimization Summary

Two licensing findings combine to yield a recurring annual saving. Figures use Microsoft published list prices as at April 2026. Actual customer pricing varies by agreement, commitment, and partner discount.

Action	Units recovered	Unit cost per month	Annual saving
Reclaim inactive E3 licences (LIC-01)	18 licences	USD 36.00	**USD 7,776.00**
Remove shared-mailbox Business Basic (EML-04)	4 licences	USD 6.00	**USD 288.00**
Total annual saving			**USD 8,064.00**

A further review of the Microsoft 365 E3 to Business Premium mix is recommended at the next contract renewal. This review is outside the scope of the current engagement.

About AroraMSP

AroraMSP is an independent Microsoft 365 consulting practice operated by Himanshu Arora. Engagements are fixed-fee and project-based. The practice focuses on tenant health audits, migration planning, security hardening, and licence optimization for organisations globally.

Credentials

• 11+ years of Microsoft ecosystem experience, including hands-on cloud support for enterprise customers across North America, Europe, and Asia Pacific.

• Microsoft 365 Certified: Administrator Expert.

• Microsoft Certified: Identity and Access Administrator Associate.

• Microsoft Certified: Azure Fundamentals.

• Microsoft Certified Solutions Expert: Productivity Solutions.

• Microsoft Certified Solutions Associate: Office 365.

Engagement model and pricing

Every engagement follows a four-step structure: discovery call, tenant audit, scoped plan, execution. Services are available across four tiers to suit organisations of every size.

`// tier 1`

USD 79 - 199

Self-serve digital products

Security checklists, PowerShell script bundles, and hardening playbooks. Instant download. Suitable for IT administrators and solo engineers who want to audit and fix their own environment.

`// tier 2`

USD 997 fixed fee

Tenant Health Audit

Five business days. Evidence-based 20-page report covering identity, email security, endpoint, collaboration, and licensing. Includes a prioritized 90-day remediation roadmap. No recurring charges.

`// tier 3`

From USD 3,500

Audit and Remediation

Audit report plus hands-on implementation of critical findings. Scoped per engagement following the audit deliverable. Suitable for organisations of 50 to 500 users.

`// tier 4`

Contact for pricing

Full project delivery

> Intune deployments, Entra ID overhauls, Exchange Online migrations, hybrid identity. Custom scoped. Suitable for 500+ user organisations, regulated industries, and government.

Contact

Website	aroramsp.com
Email	himanshu@aroramsp.com
LinkedIn	linkedin.com/in/himanshusac
GitHub	github.com/hiaror

End of report