

Microsoft 365 Security Checklist

Essential Security Settings for Australian Law Firms

This checklist covers the critical security configurations every law firm should implement in Microsoft 365 to protect client data, meet regulatory obligations, and defend against cyber threats. Work through each section systematically, ticking items as you complete them.

1. Identity & Access Management

Multi-Factor Authentication (MFA)

- **Enable MFA for all users**

Admin Center → Users → Multi-factor authentication → Enable for all accounts

- **Enforce MFA for administrators**

Azure AD → Security → Conditional Access → Require MFA for admin roles

- **Disable legacy authentication protocols (IMAP, POP3, SMTP AUTH)**

- **Configure MFA registration campaign for new users**

- **Set up authenticator app as primary MFA method**

Prefer Microsoft Authenticator or hardware keys over SMS

- **Review and remove unused MFA bypass rules**

- **Enable number matching for MFA push notifications**

Conditional Access Policies

- **Block sign-ins from high-risk locations**

Create policy blocking countries where firm has no business presence

- **Require compliant devices for access**

Ensure only managed devices can access M365 resources

- **Block access from legacy authentication clients**

- **Require MFA for risky sign-ins**

Use Azure AD Identity Protection risk-based policies

- **Restrict access to specific applications based on user role**

- **Configure session timeout policies**

Set 8-hour maximum session lifetime for sensitive apps

- **Create named locations for trusted office networks**

- **Require MFA when accessing from outside Australia**

Password & Account Security

- Disable password expiration (rely on MFA instead)
- **Enable Azure AD Password Protection**
Block common passwords and firm-specific terms
- Configure account lockout thresholds (10 failed attempts)
- **Enable Self-Service Password Reset (SSPR)**
Require two authentication methods for reset
- Review and disable unused/stale accounts monthly
- Implement Privileged Identity Management (PIM) for admin roles

2. Email Security

Email Protection & Authentication

- **Configure SPF record**
Add TXT record: v=spf1 include:spf.protection.outlook.com -all
- **Configure DKIM signing**
Enable DKIM in Microsoft 365 Defender portal
- **Configure DMARC policy**
Start with p=none, move to p=quarantine, then p=reject
- **Enable Safe Attachments**
Microsoft 365 Defender → Policies → Safe Attachments
- **Enable Safe Links**
Scan URLs in emails and Office documents
- Configure anti-phishing policies with mailbox intelligence
- Enable external email tagging/warnings
- **Block auto-forwarding to external domains**
Critical for preventing data exfiltration
- Configure spam filter policies (aggressive for legal sector)
- Enable zero-hour auto purge (ZAP) for malware and phishing
- Review quarantine policies and retention periods
 - *Email is the #1 attack vector for law firms. Prioritise these settings.*

3. Data Protection & Compliance

Data Loss Prevention (DLP)

- **Create DLP policies for sensitive information**

Target: Credit cards, TFNs, passport numbers, legal matter IDs

- Configure DLP policy tips to educate users

- **Enable DLP for Teams, SharePoint, and OneDrive**

Not just Exchange Online

- Create custom sensitive information types for client matter numbers

- Set up DLP incident reports and alerts

- **Block external sharing of files containing sensitive data**

Apply to SharePoint and OneDrive

Sensitivity Labels & Classification

- **Create sensitivity labels**

E.g., Public, Internal, Confidential, Legal Privileged

- Configure label policies and publish to users

- Enable automatic labelling for documents containing sensitive data

- **Apply encryption to Confidential and Legal Privileged labels**

Restrict access to internal users only

- Configure visual markings (headers, footers, watermarks)

- Enable mandatory labelling for documents and emails

Retention & eDiscovery

- Create retention policies for email (7 years for legal matters)

- Configure SharePoint and OneDrive retention policies

- **Enable litigation hold for relevant users/matters**

Preserve data for eDiscovery

- Set up retention labels for matter-specific retention

- Configure Teams retention policies (chat and channel messages)

- Review and document retention schedule with legal team

4. Endpoint & Device Security

Device Management & Compliance

■ Enrol all devices in Microsoft Intune

Required for Conditional Access compliance

■ Configure device compliance policies (encryption, PIN, updates)

■ Enable Microsoft Defender for Endpoint

■ Configure application protection policies

Protect M365 apps on BYOD devices

■ Block unmanaged devices from accessing sensitive data

■ Enable remote wipe capability for lost/stolen devices

■ Configure Windows Hello for Business

■ Require BitLocker encryption on Windows devices

■ Enable automatic Windows and Office updates

5. Audit, Monitoring & Response

Audit Logging

■ Enable Unified Audit Log

Microsoft Purview → Audit → Turn on auditing

■ Configure audit log retention (minimum 1 year)

■ Enable mailbox auditing for all mailboxes

■ Set up alert policies for suspicious activities

■ Configure admin activity alerts

Monitor changes to security settings

■ Enable sign-in logs retention in Azure AD

■ Review audit logs weekly for anomalies

Security Monitoring & Alerts

■ Enable Microsoft Secure Score and review recommendations

■ Configure Microsoft 365 Defender alerts

Set up email notifications for high-severity alerts

■ Enable Azure AD Identity Protection

■ Configure risky user and risky sign-in alerts

■ Set up automated investigation and response (AIR)

■ Review Threat Explorer dashboard regularly

■ Document incident response procedures for M365 security events

6. Collaboration Security (Teams, SharePoint, OneDrive)

Sharing & External Access Controls

- **Restrict external sharing in SharePoint**

Set to 'Existing guests' or 'Only people in your organisation'

- Configure sharing links to expire after 30 days

- **Disable anonymous sharing links**

Require authentication for all shared content

- Review and restrict Teams guest access policies

- Configure Teams meeting policies (lobby, recording, external participants)

- Enable Information Barriers for conflict walls (if required)

- Restrict third-party app installations in Teams

- Configure OneDrive sync restrictions to managed devices only

- Review SharePoint site permissions quarterly

- *Law firms must carefully control external collaboration to protect client confidentiality.*

7. Administrative Security

Privileged Access Management

- **Implement least-privilege access**

Use role-based access control (RBAC) for admin tasks

- Create dedicated admin accounts (separate from daily use accounts)

- Enable Privileged Identity Management (PIM) for just-in-time access

- **Require phishing-resistant MFA for all admins**

FIDO2 keys or Windows Hello

- Review admin role assignments quarterly

- Configure emergency access accounts (break-glass)

- Enable admin consent workflow for third-party apps

- Block admin accounts from email and Teams

- Monitor admin activity with dedicated alert policies

CHECKLIST COMPLETION RECORD

Completed by:	
----------------------	--

Date:	
Reviewed by:	
Next review date:	

Need help implementing these controls? Cyooda Security specialises in cybersecurity for Australian law firms. Contact us for a security assessment or to discuss your Microsoft 365 security posture. Visit www.cyooda.com or email info@cyooda.com