Free Essential Eight (Maturity Level 1) Cybersecurity Checklist

For Small Businesses – Download & Implement Today

This **comprehensive checklist** helps you implement the **ACSC Essential Eight** at **Maturity Level One**—the baseline cybersecurity standard for Australian small businesses.

✅ Multi-Factor Authentication (MFA)

🔷 Enable MFA for all critical systems:

- Email (Office 365, Google Workspace)
- Cloud storage (OneDrive, Dropbox, SharePoint)
- Banking & financial apps
- Remote access (VPN, RDP)

🔷 Best Practices:

- Use an **authenticator app** (Google/Microsoft Authenticator) instead of SMS where possible.
- Train staff to **recognize MFA fatigue attacks** (repeated push notifications).

✅ Patch Applications & Operating Systems

🔷 Turn on automatic updates for:

- Windows/macOS
- Web browsers (Chrome, Edge, Firefox)
- Plugins (Java, Adobe, Zoom)

🔷 Critical Actions:

- Replace **end-of-life software** (e.g., Windows 7).
- Patch **within 48 hours** for critical vulnerabilities.

✅ Daily Backups (3-2-1 Rule)

🔷 Backup Requirements:

- **3 copies** of data (1 primary + 2 backups)
- **2 different storage types** (e.g., cloud + external drive)
- **1 offline backup** (protects against ransomware)

🔷 **Backup Testing:**

- Test **restores quarterly** to ensure backups work.
- Encrypt backups to protect sensitive data.

✅ **Application Control**

🔷 **Block unauthorized software:**

- Use **allowlisting** to only permit approved apps.
- Deny installations by standard users.

🔷 **High-Risk Apps to Block:**

- Pirated/cracked software
- Unverified portable apps (e.g., USB executables)

✅ **Restrict Administrative Privileges**

🔷 **Limit admin access:**

- Only **necessary staff** have admin rights.
- Use **standard accounts** for daily tasks.

🔷 **Monitor Admin Activity:**

- Log all admin actions (who, what, when).

✅ **Configure Microsoft Office Macros**

🔷 **Macro Security:**

- Block macros from **internet/downloaded files**.
- Only allow **signed macros** from trusted sources.

✅ **User Application Hardening**

🔷 **Disable risky features:**

- Flash Player
- Java (unless explicitly needed)
- Unnecessary browser plugins

✅ **Logging & Monitoring**

🔷 **Enable basic logging:**

- Failed login attempts
- Admin account changes
- Unusual file access

🔷 **Retention Policy:**

- Store logs for **at least 3 months**.