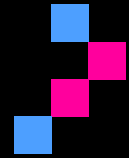


Ransomware Readiness Checklist



Initial
TECH

Overview

This plain-English checklist helps small and mid-market clients prepare for, withstand, and recover from ransomware. It combines guidance from ACSC, CISA, NIST CSF 2.0 and Microsoft, and uses the same easy tick-box style as the Essential Eight template.

How to use this checklist

- 1) Work through each section, ticking Status and pasting screenshots or links under Evidence.
- 2) Capture gaps in the Action plan with owners and due dates.
- 3) Test backups and run an incident tabletop quarterly.
- 4) Revisit after personnel, system, or vendor changes.

Quick Wins (do these first)

- Never pay a ransom; report incidents and get help via 1300 CYBER1 / ReportCyber.
- Enforce MFA for all accounts (admins first), and block legacy authentication.
- Enable email protections (Safe Links, Safe Attachments, anti-phishing) and external forwarding blocks.
- Adopt 3-2-1-1-0 backups with one immutable/offline copy; test restores.
- Keep software/firmware patched; remove end-of-life systems.

1. Governance & scope

Set clear ownership, legal obligations, and scope for ransomware readiness, aligned to NIST CSF 2.0 (Govern/Identify).

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Name an incident lead and deputies	Assign roles (lead, comms, technical, legal/insurance); publish contact tree.		
Document legal/reporting obligations	List ACSC hotline, ReportCyber steps, sector rules (e.g., SOCI, privacy).		
Inventory critical data, systems and vendors	Identify where crown-jewel data lives and who has access; include cloud apps.		
Approve a quarterly tabletop schedule	Run, record learnings, and update the plan.		

2. Prevent initial access (accounts, email, endpoints)

Close common entry points: weak credentials, phishing, and unprotected endpoints.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Enforce MFA for all users/admins	Use app-based MFA or passkeys; prioritise email, VPN/remote, privileged roles.		
Block legacy authentication	Create Conditional Access policy to block basic/legacy protocols.		
Harden email & collaboration	Apply Defender preset policies (Standard/Strict), Safe Links/Attachments, anti-phishing; block auto-forward.		
Deploy EDR/AV to all devices	Use reputable EDR; enable isolation/rollback; monitor coverage.		
Patch OS/apps/firmware fast	Critical fixes within 14 days; maintain compliance reports.		

3. Limit spread (Zero Trust controls)

Reduce lateral movement and data exposure if an attacker gets in.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Conditional Access & device compliance	Require MFA + compliant devices; block risky sign-ins and geographies.		
Least privilege & admin separation	Minimise Global Admins; use PIM/JIT; separate backup admin identities.		
Restrict external sharing and downloads	Tighten SharePoint/OneDrive; use DLP/sensitivity labels; session controls on unmanaged devices.		
Email authentication (SPF/DKIM/DMARC)	Publish and monitor records to cut spoofing and BEC.		

4. Backups & recovery (3-2-1-1-0)

Guarantee clean recovery without paying. Keep one offline/immutable copy and verify restores.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Follow 3-2-1-1-0	3 copies, 2 media, 1 offsite, 1 immutable/offline, 0 errors via regular restore tests.		
Separate backup credentials & networks	Use distinct accounts/keys; limit console access; consider isolated network/tenant.		
Enable Microsoft 365 versioning/File Restore	Ensure ≥500 versions, 93-day recycle bin, and OneDrive/SharePoint File Restore.		
Quarterly full-restore drills	Measure RTO/RPO; document outcomes; fix bottlenecks.		

5. Detection & response playbook

Write a step-by-step playbook: contain, eradicate, restore, and report.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Immediate containment steps	Isolate infected hosts; disable accounts; stop external sharing; block C2 domains.		
Forensics & evidence	Capture images/memory; preserve logs; record ransom notes/IOCs.		
Law enforcement & reporting	Call 1300 CYBER1; lodge ReportCyber; notify regulators/insurer as required.		
Restore & validate	Recover from clean, immutable backups; validate integrity before go-live.		
Post-incident review	Root cause, lessons learned, control updates, user comms.		

6. Cyber insurance & compliance readiness

Collect evidence insurers and auditors ask for to avoid denial and reduce premiums.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Proof of MFA/EDR/backups	Screenshots/reports showing enforcement and immutability; restore test records.		
Patch compliance and exceptions	Monthly reports; documented mitigations for exceptions.		
Incident response plan & tabletop records	Dated plans, contact lists, exercise minutes and improvements.		
Vendor security & data location	Contracts/attestations; critical supplier controls and contacts.		

Action plan (next steps)

Action	Owner	Due date	Resources	Status

References

- ACSC Ransomware Emergency Response Guide & Report/Recover pages
- Microsoft ransomware protection (tenant/service), backup/restore plans
- CISA Ransomware Response Checklist & advisories (e.g., Play ransomware)
- NIST CSF 2.0 Small Business Quick-Start & ransomware profile (NISTIR 8374 Rev. 1 draft)
- Backup best practices: 3-2-1-1-0, immutable/offline copies, restore testing (NCSC/Veeam/industry)