LucidSeal

Template: Baseline Cyber Hygiene Checklist

A quick, confidence-building checklist for keeping your people, data, and devices secure.

Doc ID	LS-TEM-0007	**Owner**	Bryan Chetcuti
Version	V1.0	**Status**	Approved
Confidentiality	Public	**Last Updated**	2025-11-07
Approver	Bryan Chetcuti	**Next Review**	2026-06-30

Change Log

Date	Author	Change	Version
2025-11-07	Bryan Chetcuti	Approved	V1.0

Template: Baseline Cyber Hygiene Checklist

This checklist helps small teams, community groups, and charities to keep systems secure, data protected, and people confident. Tick what's in place - what's left blank becomes your next quick win.

Tips for Use: *Start small: aim to complete one section each week, and celebrate every box you tick - progress matters more than perfection.*

Review this checklist every six months or after major system changes to track progress and demonstrate accountability.

Use it as a team activity - discuss each item together, agree what's "in place," and note where support or training might help.

Print a copy for your next meeting - ticking boxes together turns cybersecurity into a shared responsibility

 1 Identity & Access

☐ All accounts use strong passwords or passphrases

☐ Multi-factor authentication (MFA) enabled on email, cloud, and admin logins

☐ Shared or generic accounts removed or renamed to individual users

☐ Admin access limited and reviewed quarterly

☐ Default credentials changed on all devices and apps

 2 Device & Patch Management

☐ Automatic updates enabled on all computers and phones

☐ Operating systems supported and not end-of-life

☐ Endpoint protection active and centrally monitored

☐ Screens auto-lock after short idle time

☐ Retired devices securely wiped before reuse or disposal

3 Cloud & Data Storage

☐ Data stored only in approved cloud or server locations
☐ Access granted by role and least-privilege principles
☐ Backups run automatically and tested twice a year
☐ Version history enabled in key apps (e.g. OneDrive, Google Drive)
☐ Sensitive data encrypted in transit and at rest

4 Email & Communication

☐ Spam and phishing filters enabled
☐ Staff trained to spot suspicious links or attachments
☐ External-sender banner or warning active
☐ Domain protected with SPF, DKIM, and DMARC
☐ No personal email used for organisation logins

5 Website & Public Presence

☐ HTTPS enforced with valid SSL certificate
☐ CMS and plugins kept up to date
☐ Admin areas protected by MFA or IP restriction
☐ Forms protected by CAPTCHA or Turnstile
☐ Privacy and Trust pages reviewed annually

6 Data Protection & Privacy

☐ Privacy policy clear and accessible
☐ Only necessary personal data collected and retained
☐ Retention periods defined and applied
☐ Sensitive information not shared via email or chat
☐ Incident or breach response plan documented

7 People & Awareness

☐ Cyber awareness included in onboarding
☐ Annual refresher or phishing simulation
☐ Clear reporting path for suspicious activity
☐ Leaders model secure behaviour
☐ Culture encourages learning not blame

8 Resilience & Recovery

☐ Critical systems identified and prioritised
☐ Backups stored off-site or separate tenant
☐ Response contacts (current IT, vendors, regulators) verified
☐ Recovery drills run periodically
☐ Lessons learned recorded and shared

9 Governance & Improvement

☐ Cyber responsibilities formally assigned
☐ Checklist reviewed every six months
☐ Progress tracked in risk or action register
☐ External guidance sources monitored (ACSC, OAIC, NIST Lite)
☐ Trust updates shared openly with stakeholders

Next Steps

1. Mark gaps as “to-do”
2. Prioritise high-impact, low-effort actions
3. Re-check quarterly - steady improvement builds resilience