CyberHouse Solutions

MANAGED IT · CYBERSECURITY · AI AUTOMATION

FREE SECURITY CHECKLIST

20-Point Microsoft 365 Security Checklist

A practical checklist for reviewing the Microsoft 365 security settings and identity protections most small businesses overlook.

Practical security organization guidance. Not legal, insurance, or compliance advice.

> This is not a full Microsoft 365 audit. Use it to catch the most common gaps first, then prioritize from there.

1 Identity & Sign-In

- [ ] Multi-factor authentication (MFA) is required for every user, including admins.
- [ ] Legacy authentication protocols (older sign-in methods that skip MFA) are blocked.
- [ ] Conditional Access policies are configured for high-risk sign-in scenarios.
- [ ] Microsoft's Security Defaults are enabled, or Conditional Access is configured as a replacement.
- [ ] Self-service password reset is enabled and configured securely.

2 Admin Roles & Guest Access

- [ ] The Global Admin role is limited to as few accounts as possible.
- [ ] Privileged admin roles are reviewed on a regular schedule.
- [ ] Guest user accounts are reviewed and removed when no longer needed.
- [ ] Guest access to sensitive Teams, SharePoint, and OneDrive content is restricted appropriately.

3 Threat Protection & Mail Flow

- [ ] Microsoft Defender (or equivalent) threat protection is enabled for email and collaboration tools.
- [ ] Anti-phishing and anti-spoofing policies are active.
- [ ] Mail flow rules are reviewed for unauthorized forwarding or unusual routing.
- [ ] Safe Links and Safe Attachments protections are enabled where available.
- [ ] Shared mailboxes are reviewed for who has access and why.

4 Password & Identity Hygiene

- [ ] Password policies follow modern guidance (length over frequent forced resets).
- [ ] Inactive or unused user accounts are disabled or removed.
- [ ] Sign-in logs are reviewed periodically for unusual or risky activity.
- [ ] Break-glass emergency admin accounts exist and are tested.

5 Microsoft Secure Score

- [ ] The organization's Microsoft Secure Score is reviewed at least quarterly.
- [ ] Top recommended Secure Score improvements are assigned an owner and a timeline.

Your Score

0–8	High risk. Start with MFA, legacy authentication, and admin role cleanup.
9–15	Moderate risk. Tighten mail flow rules, guest access, and Secure Score follow-through.
16–20	Better than most small businesses. Review quarterly.

WHAT'S NEXT

Whether you prefer to do it yourself or work with an expert, the goal is the same: reduce your risk before it becomes a business problem.

DIY PATH

Want the expanded tracker, policy templates, vendor inventory, backup checklist, and first-24-hours incident response worksheet?

Get the Starter Kit →

DONE-WITH-YOU PATH

Prefer an expert to review your Microsoft 365 environment and fix the highest-risk items directly?

Book a Microsoft 365 Email Security Review →