

The UK Small Business Microsoft 365 Security Checklist 2026

A practical checklist informed by NCSC, Microsoft and relevant Cyber Essentials guidance.

40 checks across eight control areas to help you understand what is configured, what needs evidence and what should happen next.

Use this with your in-house IT team, MSP or IT provider. You do not need to be technical: ask the question, request the evidence and record the next action.

Organisation:

Review date:

Business reviewer:

IT provider / technical reviewer:

Scope: people, devices, domains and Microsoft 365 services included:

Exclusions or unavailable data:

How to use the checklist

1. Agree the scope before checking anything.
2. For each control, ask for dated evidence that covers that scope.
3. Circle one status and record an evidence reference or next action.
4. Agree owners and dates for the most important gaps on page 10.

V — Verified: evidence was reviewed and supports the control.

A — Action needed: an issue needs investigation or remediation.

E — Evidence needed: you cannot establish the answer yet.

N — Not applicable: record the reason; do not assume a pass.

An unanswered item means “not established”, not “secure”. Keep evidence securely; do not collect passwords, recovery codes or API secrets.

Identity & MFA

Check who can sign in and how access is protected. MFA registration alone does not establish enforcement.

Check	Why it matters	How to verify / evidence to request	Status
1. MFA coverage for all users	Stolen passwords can give attackers access.	Review Entra authentication-method reports plus Security Defaults or Conditional Access targeting, exclusions and sign-in evidence.	V / E A / N
Evidence reference / next action: _____			
2. Stronger MFA for privileged accounts	An administrator compromise has greater impact.	Review authentication-strength policies and supported phishing-resistant methods for administrators; document exceptions.	V / E A / N
Evidence reference / next action: _____			
3. Legacy authentication blocked	Older sign-in methods can avoid modern protections.	Review Security Defaults or Conditional Access and legacy-authentication sign-in activity; identify dependencies before changes.	V / E A / N
Evidence reference / next action: _____			
4. Access policies deliberately configured	Gaps in policy scope leave users unprotected.	Identify whether Security Defaults or Conditional Access is used; review policy state, targeted users, applications and exclusions.	V / E A / N
Evidence reference / next action: _____			
5. Inactive accounts and leavers reviewed	Unneeded accounts remain an entry point.	Review inactive identities and recent leavers, including provider accounts, sessions and access-removal records.	V / E A / N
Evidence reference / next action: _____			

Supporting guidance: [Identity & MFA — official guidance](#). See methodology on page 11.

Administrator security

Know who can change your organisation's services, why they need that access and how access can be recovered.

Check	Why it matters	How to verify / evidence to request	Status
6. Global Administrator access reviewed	Broad privileges increase the impact of mistakes or compromise.	Review active, eligible and group-based role assignments and named owners. Microsoft recommends fewer than five Global Administrators; document business need.	V / E A / N
Evidence reference / next action: _____			
7. Least privilege used	Routine work rarely needs full administrator access.	Compare assigned roles with actual duties; use narrower roles and time-limited privileges where supported.	V / E A / N
Evidence reference / next action: _____			
8. Separate administrator accounts	Daily email and browsing expose privileged identities.	Review account inventories and the IT provider's procedure; keep privileged identities separate from everyday work.	V / E A / N
Evidence reference / next action: _____			
9. Emergency access arrangements tested	Policy changes or outages can lock out administrators.	Review protected emergency accounts, monitoring and a dated access test; document how authorised people recover access.	V / E A / N
Evidence reference / next action: _____			
10. Provider privileges periodically reviewed	Supplier access can persist after the reason has ended.	Review delegated and guest administration, MFA protection, access scope and last review; assign an internal owner.	V / E A / N
Evidence reference / next action: _____			

Supporting guidance: [Administrator security — official guidance](#). See methodology on page 11.

Email security

Review both domain authentication and mailbox behaviour. A DNS record alone does not prove the complete email configuration.

Check	Why it matters	How to verify / evidence to request	Status
11. SPF, DKIM and DMARC reviewed	Domain impersonation undermines trust in business email.	Review DNS for each sending domain, authorised senders, DKIM signing, DMARC policy and reports; account for third-party senders.	V / E A / N
Evidence reference / next action: _____			
12. External forwarding controlled	Mail can leave the organisation without users noticing.	Review Exchange outbound forwarding policies and exceptions, mailbox forwarding and inbox rules; establish approved destinations.	V / E A / N
Evidence reference / next action: _____			
13. Anti-phishing protections reviewed	Impersonation can lead to credential theft or payment fraud.	Review applicable Defender or Exchange policies, coverage and exceptions; record licence-dependent protections.	V / E A / N
Evidence reference / next action: _____			
14. Suspicious mailbox rules investigated	An attacker may hide or redirect messages.	Request a dated rule and forwarding review, relevant alerts and investigation outcomes; document legitimate exceptions.	V / E A / N
Evidence reference / next action: _____			
15. Payment changes independently confirmed	A convincing email can still be fraudulent.	Review the finance procedure and a recent example of verifying bank-detail changes by callback to a known number.	V / E A / N
Evidence reference / next action: _____			

Supporting guidance: [Email security — official guidance](#). See methodology on page 11.

Sharing & collaboration

Understand which people outside the organisation can see information, and how long access lasts.

Check	Why it matters	How to verify / evidence to request	Status
16. SharePoint and OneDrive sharing reviewed	Oversharing can expose business or customer information.	Review organisation, site and OneDrive sharing settings, permitted domains and actual external access.	V / E A / N
Evidence reference / next action: _____			
17. Anonymous links restricted appropriately	Anyone with a link may be able to access information.	Review default link types, Anyone-link permissions and expiry where supported; sample links containing sensitive information.	V / E A / N
Evidence reference / next action: _____			
18. Guest accounts regularly reviewed	Old relationships can leave unnecessary access behind.	Review guest identities, owners, memberships and activity; record decisions to retain or remove access.	V / E A / N
Evidence reference / next action: _____			
19. Teams guest and external access reviewed	Collaboration settings affect who can interact with staff.	Review Teams guest access, external access, allowed domains and relevant meeting policies; distinguish chat access from file access.	V / E A / N
Evidence reference / next action: _____			
20. Sensitive data sharing has an owner	No one may notice when access becomes inappropriate.	Identify sensitive sites and files, responsible owners and a dated access review; document how sharing concerns are raised.	V / E A / N
Evidence reference / next action: _____			

Supporting guidance: [Sharing & collaboration — official guidance](#). See methodology on page 11.

Applications & permissions

Applications may retain access independently of a user's password. Review what they can access and who approved it.

Check	Why it matters	How to verify / evidence to request	Status
21. Third-party applications inventoried	Unknown applications may hold access to business data.	Review Entra enterprise applications and app registrations; identify owners, purpose and the approval record.	V / E A / N
Evidence reference / next action: _____			
22. Permissions proportionate to need	Excessive permissions increase the impact of compromise.	Review delegated and application permissions, tenant-wide consent and privileged grants; ask the owner to justify sensitive access.	V / E A / N
Evidence reference / next action: _____			
23. User consent deliberately restricted	Users may approve data access without understanding it.	Review user-consent policies and the administrator approval workflow; establish who reviews requests.	V / E A / N
Evidence reference / next action: _____			
24. Unused applications and grants reviewed	Abandoned integrations can retain usable access.	Review app usage, ownership and outstanding grants; investigate before removing dependencies.	V / E A / N
Evidence reference / next action: _____			
25. Application credentials responsibly managed	Unmanaged secrets can expose long-lived access.	Review credential owners, expiry, rotation and secure storage; request inventory evidence, never the secret values.	V / E A / N
Evidence reference / next action: _____			

Supporting guidance: [Applications & permissions — official guidance](#). See methodology on page 11.

Devices

Include remote and personally owned devices where relevant. Microsoft 365 settings cannot establish every device's condition.

Check	Why it matters	How to verify / evidence to request	Status
26. Devices known and management agreed	Unknown devices are difficult to protect or recover.	Review the device inventory, ownership, management coverage and BYOD rules; record devices outside management.	V / E A / N
Evidence reference / next action: _____			
27. Operating systems and software supported	Unsupported software stops receiving necessary fixes.	Request operating-system and application inventories, support status and plans for unsupported exceptions.	V / E A / N
Evidence reference / next action: _____			
28. Security updates applied	Known vulnerabilities can remain exploitable.	Review dated update reports, overdue fixes and owners; include remote devices and business applications.	V / E A / N
Evidence reference / next action: _____			
29. Endpoint protection and firewalls active	Malware and unwanted network access can disrupt work.	Review protection health, alerts and device firewall configuration; document exceptions and supported coverage.	V / E A / N
Evidence reference / next action: _____			
30. Encryption and lost-device response established	Lost devices can expose stored business information.	Review encryption evidence and lost/stolen-device procedures, including remote actions where available and personal-device limits.	V / E A / N
Evidence reference / next action: _____			

Supporting guidance: [Devices — official guidance](#). See methodology on page 11.

Backup & recovery

Identify the data you need to keep operating. Retention, synchronisation and a backup are not automatically interchangeable.

Check	Why it matters	How to verify / evidence to request	Status
31. Critical data and recovery needs identified	Recovery may miss the information the business needs.	List critical email, files, records and services; agree tolerable data loss, downtime and responsible owners.	V / E A / N
Evidence reference / next action: _____			
32. Backup coverage documented	A service may exclude important data or retain it too briefly.	Review backup scope, frequency, retention, exclusions and recovery arrangements for relevant Microsoft 365 services.	V / E A / N
Evidence reference / next action: _____			
33. Backup access protected	Attackers may delete or compromise recovery copies.	Review backup administrator MFA, least privilege, deletion protection and separation from everyday access where supported.	V / E A / N
Evidence reference / next action: _____			
34. Representative restores completed	A configured backup may not be usable when needed.	Request a dated test showing data restored, completeness, time taken, outcome and unresolved issues.	V / E A / N
Evidence reference / next action: _____			
35. Recovery responsibilities understood	Unclear ownership delays recovery during disruption.	Review the recovery runbook, provider commitments, escalation contacts and access to instructions when normal services are unavailable.	V / E A / N
Evidence reference / next action: _____			

Supporting guidance: [Backup & recovery — official guidance](#). See methodology on page 11.

Monitoring & governance

Make checking a repeatable business process, with named people reviewing findings and evidence.

Check	Why it matters	How to verify / evidence to request	Status
36. Secure Score reviewed in context	A percentage can hide important gaps or assumptions.	Review dated recommendations, accepted risks and owners. Secure Score measures posture and does not cover every attack surface.	V / E A / N
Evidence reference / next action: _____			
37. Suspicious sign-ins and alerts reviewed	Warning signs need someone to investigate them.	Review sign-in logs, available risk detections, alert coverage and investigation records; note licence and retention limits.	V / E A / N
Evidence reference / next action: _____			
38. Audit evidence accessible	Missing logs can prevent effective investigation.	Review directory and mailbox audit settings separately, retention, access rights and a recent search example.	V / E A / N
Evidence reference / next action: _____			
39. Review schedule and evidence retained	Settings and responsibilities change over time.	Agree periodic account, role, application and sharing reviews; retain dated evidence with reviewer, scope and exceptions.	V / E A / N
Evidence reference / next action: _____			
40. Incidents and corrective actions owned	An unresolved finding can remain a business risk.	Review incident contacts and an action register with owner, target date, risk decisions and evidence of completion.	V / E A / N
Evidence reference / next action: _____			

Supporting guidance: [Monitoring & governance — official guidance](#). See methodology on page 11.

Agree your next three priorities

Do not close an evidence gap until someone has reviewed the evidence. Assign an owner and target date for each important finding.

Check / finding	Next action / evidence needed	Owner	Target date

Evidence reviewer:

Next review date:

Copy this request to your IT provider

Please provide dated evidence for checklist item ____ covering _____.

Include the configuration or report, scope, exclusions and review or test outcome. Identify anything that could not be established and any action required.

Use our agreed secure upload route. Do not send passwords, recovery codes or API secrets.

What CyberProva can help with

Selected read-only checks can verify supported Microsoft 365 settings. Evidence requests help gather material for controls requiring your IT provider. Your organisation reviews that evidence.

Configuration checks do not prove every user’s MFA enforcement, every device’s security, successful recovery or the absence of compromise. Licences, consent and data availability affect coverage.

Put the checklist to work

Keep selected automated findings and provider evidence alongside your priorities. Free includes three lifetime core assessments; exports and advanced features require a paid plan.

[Run your free Microsoft 365 security assessment →](#)

How this checklist was developed

CyberProva reviewed public NCSC and Microsoft guidance and relevant Cyber Essentials requirements, then selected and simplified practical questions for small organisations using Microsoft 365. This is a selective worksheet, not a complete technical benchmark.

Foundation and supporting sources

- [NCSC Small Organisations Guide](#): email, accounts, devices, backups and recognising attacks. The [backup guidance](#) informs recovery checks 31–35.
- [Microsoft secure sign-in guidance](#), [Security Defaults](#) and [administrator best practices](#) support identity and access checks 1–10. Each control area links to further official guidance.
- [Cyber Essentials requirements for IT infrastructure v3.3](#), effective 27 April 2026: relevant baseline themes are mapped below. The checklist does not assess the full requirements or certification scope.
- [Microsoft Secure Score](#) informs check 36. It is a posture measure, not complete assurance or a guarantee against compromise.

Relevant Cyber Essentials themes

User access control: checks 1–10 and application access in 21–23.

Secure configuration: relevant access and application settings in 4, 21–23 and device management in 26.

Security updates: checks 27–28.

Malware protection: check 29.

Firewalls: device firewall evidence in check 29. Network boundary coverage requires a separate review.

These are thematic connections, not a requirement-by-requirement compliance mapping. Backups, monitoring and other useful checks extend beyond the five Cyber Essentials technical control areas.

Where CIS fits

The [CIS Microsoft 365 Foundations Benchmark](#) is useful further reading for a deeper technical configuration review. This worksheet has not been mapped to or validated against the full CIS benchmark and does not claim CIS compliance or endorsement.

Use the result responsibly

This resource is not an audit, certification, penetration test or guarantee of security or insurance cover. Cyber Essentials certification requires its own assessment through a Certification Body. Record exceptions, unavailable evidence and review dates; recheck controls after important changes.

CyberProva can verify many of these controls automatically.