PCC

PROFESSIONAL COMPUTER CONCEPTS

Microsoft 365 security guidance for small businesses

Microsoft 365 Security Checklist for Small Businesses

Use this worksheet to review identity, administrator access, email, file sharing, devices, backup, monitoring, and employee preparedness.

How to use this worksheet

- Review each line with the person responsible for Microsoft 365 administration.
- Mark one status: Complete, Needs Review, or Not Available.
- Record an owner and target date for items requiring action.
- Mark unavailable licensed controls N/A, then evaluate whether the gap matters.

Assessment details

Organization

Reviewer

Assessment date

Microsoft 365 plan / license

Identity and Administrator Protection

Select one status for each item. Use the notes area to document gaps and next actions.

Identity and Sign-In Protection	COMPLETE	REVIEW	N/A
Require multifactor authentication for every active user account.	☐	☐	☐
Use stronger authentication methods such as Authenticator, passkeys, or security keys where possible.	☐	☐	☐
Use Security Defaults or properly designed Conditional Access policies.	☐	☐	☐
Block outdated legacy authentication unless a documented exception is required.	☐	☐	☐
Review inactive, guest, and shared accounts regularly.	☐	☐	☐

Administrator Protection	COMPLETE	REVIEW	N/A
Give each administrator a separate account reserved for administrative work.	☐	☐	☐
Limit Global Administrator access and use least-privileged roles.	☐	☐	☐
Require strong, preferably phishing-resistant MFA for privileged accounts.	☐	☐	☐
Review administrator role assignments on a defined schedule.	☐	☐	☐
Maintain and monitor a documented emergency-access process.	☐	☐	☐

Section owner / notes

Email, Files, and Permissions

Select one status for each item. Use the notes area to document gaps and next actions.

Email Security

	COMPLETE	REVIEW	N/A
Configure SPF, DKIM, and DMARC for every domain that sends company email.	☐	☐	☐
Review anti-phishing, anti-spam, and malware protection policies.	☐	☐	☐
Protect frequently impersonated employees and trusted business domains.	☐	☐	☐
Enable Safe Links and Safe Attachments when supported by licensing.	☐	☐	☐
Block unnecessary automatic forwarding to external addresses.	☐	☐	☐
Give employees a clear, monitored method for reporting suspicious email.	☐	☐	☐

Files and Permissions

	COMPLETE	REVIEW	N/A
Define when employees may share company information externally.	☐	☐	☐
Restrict anonymous Anyone links or apply expiration and limited permissions.	☐	☐	☐
Keep sensitive information in sites where external sharing is disabled.	☐	☐	☐
Review site owners, Teams membership, guests, and sharing links regularly.	☐	☐	☐
Use named recipients and view-only access whenever practical.	☐	☐	☐
Evaluate sensitivity labels and data-loss prevention for sensitive information.	☐	☐	☐

Section owner / notes

Devices, Applications, and Recovery

Select one status for each item. Use the notes area to document gaps and next actions.

Devices and Applications

	COMPLETE	REVIEW	N/A
Maintain an accurate inventory of devices accessing Microsoft 365.	☐	☐	☐
Keep operating systems, browsers, and Microsoft 365 applications patched.	☐	☐	☐
Require encryption, automatic screen locks, and endpoint protection.	☐	☐	☐
Evaluate device compliance and Conditional Access when licensed.	☐	☐	☐
Define security requirements for personal devices accessing company data.	☐	☐	☐
Review third-party OAuth applications and remove unnecessary permissions.	☐	☐	☐

Backup and Recovery

	COMPLETE	REVIEW	N/A
Document which Exchange, OneDrive, SharePoint, and Teams data requires backup.	☐	☐	☐
Use Microsoft 365 Backup or a qualified third-party backup solution.	☐	☐	☐
Do not treat retention policies or recycle bins as a complete backup strategy.	☐	☐	☐
Protect backup administration with strong authentication and limited access.	☐	☐	☐
Monitor backup status, coverage, failures, and newly created accounts or sites.	☐	☐	☐
Test recovery of email, files, and SharePoint content before an emergency.	☐	☐	☐

Section owner / notes

Monitoring, Training, and Action Plan

Monitoring and Employee Training	COMPLETE	REVIEW	N/A
Monitor risky sign-ins and unusual account activity.	☐	☐	☐
Monitor administrator changes, mailbox rules, forwarding, and app permissions.	☐	☐	☐
Use Microsoft Secure Score as an input, not as the definition of security.	☐	☐	☐
Document responsibilities and procedures for Microsoft 365 incidents.	☐	☐	☐
Provide recurring security-awareness training for all employees.	☐	☐	☐
Use phishing simulations to measure reporting and improvement over time.	☐	☐	☐
Maintain reliable onboarding, role-change, and offboarding procedures.	☐	☐	☐

Priority action plan

Priority gap	Owner	Target date

Need help turning the findings into a security plan?

Professional Computer Concepts helps Bay Area businesses secure and manage Microsoft 365.

calpcc.com/contact-us/ | 415-897-0078