

Small Business Cybersecurity Checklist

Mark a check after reviewing the evidence. Assign open items an owner and date. This is a planning aid, not a certification.

☐ 01 Identify the essential services

List the applications, devices and information needed to serve customers, pay staff and keep records. Name the person responsible for each.

Evidence: A dated service list with named owners.

Owner

Target date

☐ 02 Review who can sign in

Check active staff, administrator and supplier accounts. Remove access that is no longer needed through your normal approval process.

Evidence: An access review and a record of agreed changes.

Owner

Target date

☐ 03 Protect high-value accounts

Prioritize multi-factor authentication for business email, administration and other important services. Confirm how each account can be recovered.

Evidence: An MFA coverage list with exceptions assigned to an owner.

Owner

Target date

☐ 04 Give updates an owner

Agree who monitors vendor updates, deploys relevant security fixes and checks completion. Record a plan for unsupported devices or software.

Evidence: An update report and an exception list.

Owner

Target date

☐ 05 Check device protection

Confirm that business devices have supported security protection and that alerts reach someone who can respond.

Evidence: A current device-protection status report.

Owner

Target date

☐ 06 Reduce unnecessary privileges

Use ordinary accounts for everyday work. Reserve administrator access for approved tasks and protect those accounts separately.

Evidence: A list of administrative accounts and their owners.

Owner

Target date

Small Business Cybersecurity Checklist

Continue the review. Record the result, including gaps and decisions that need follow-up.

☐ 07 Identify information that needs backup

Confirm which business information is covered, including relevant cloud services. Set a backup frequency that fits how quickly the information changes.

Evidence: A backup scope and schedule agreed by the business.

Owner

Target date

☐ 08 Prove a small restore works

Plan an authorized test using a separate location or test environment. Recover a sample and confirm it can be opened without replacing live information.

Evidence: A dated restore result and a record of any gaps.

Owner

Target date

☐ 09 Make reporting easy

Tell staff how to report suspicious messages or unexpected sign-in requests. Provide a trusted contact method they can find quickly.

Evidence: A reporting instruction shared with the team.

Owner

Target date

☐ 10 Keep essential incident contacts accessible

Record who coordinates an incident and how to reach IT support and other relevant partners if normal systems are unavailable.

Evidence: An accessible contact sheet with a review date.

Owner

Target date

☐ 11 Understand supplier responsibilities

Ask important cloud and IT suppliers who handles updates, backups, account recovery and incident communication. Record the boundaries of your own responsibilities.

Evidence: A responsibility summary for critical services.

Owner

Target date

☐ 12 Choose the next three improvements

Select three unresolved items, assign an owner and target date, and agree when progress will be reviewed.

Evidence: A short action plan with owners and dates.

Owner

Target date

Turn checks into next steps.

For business owners and small teams planning routine improvements. Schedule system changes with the person responsible for your IT.

YOUR BUSINESS REVIEW

Review led by Date

Next review

NEXT THREE ACTIONS / OWNER / TARGET DATE

Sources and scope

Cyber Centre: Foundational security actions (ITSAP.10.300)

<https://www.cyber.gc.ca/en/guidance/foundational-cyber-security-actions-small-organizations-itsap10300>

Cyber Centre: Baseline controls for small and medium organizations

<https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations>

Cyber Centre: How updates secure your device (ITSAP.10.096)

<https://www.cyber.gc.ca/en/guidance/how-updates-secure-your-device-itsap10096>

Get Cyber Safe: Cyber security checklist

<https://www.getcybersafe.gc.ca/en/resources/cyber-security-checklist>

Prepared by Canada NexTech. Source guidance checked October 28, 2026. This independent educational resource is not endorsed by the source organizations. Adapt it with the person responsible for your systems.