

Small Business Cyber Readiness

A starting checklist for a small team. Assign an owner and test each control. Tailor the plan to your systems, legal duties, and service needs.

Know what matters

- ☐ **List important accounts, services, devices, and vendors.**
Record an owner and a backup contact for each critical service.
- ☐ **Identify the work that cannot stop.**
Write down essential data, dependencies, and a manual workaround.

Reduce common entry points

- ☐ **Require MFA for email, remote access, and administrators.**
Review who has privileged access and remove accounts no longer needed.
- ☐ **Update exposed systems and supported software.**
Prioritize known exploited weaknesses and test changes before broad rollout.
- ☐ **Keep protected backups and test a restore.**
Record the last successful restore, how long it took, and what was missing.
- ☐ **Teach a separate verification path for payment and data requests.**
A familiar voice, email address, or logo alone is not proof of identity.

Prepare a response

- ☐ **Name the people who can contain an incident.**
Include after-hours decision makers, your IT provider, and key vendors.
- ☐ **Keep a copy of the response plan outside the affected systems.**
Include how to preserve logs and who approves shutdowns or notifications.
- ☐ **Run one tabletop exercise and record follow-up work.**
Practice both a security decision and an operations decision.

Sources and further guidance

[CISA StopRansomware Guide](https://www.cisa.gov/stopransomware/ransomware-guide) | <https://www.cisa.gov/stopransomware/ransomware-guide>

[CISA Secure Your Business](https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business) | <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business>