K

Small Business Cyber Security Checklist

54 yes-or-no checks for your office, website, servers and apps built with AI coding tools, mapped to the CIS Critical Security Controls v8.1 (Implementation Group 1) and the NIST Cybersecurity Framework 2.0.

How to use it
Tick a box only when you have checked the real thing, not what someone remembers or what a settings page claims.

CIS v8.1
The safeguard numbers each check covers. "beyond IG1" marks checks we add because they matter for small businesses today.

NIST CSF 2.0
The framework function: Govern, Identify, Protect, Detect, Respond or Recover.

Small office 25 checks

Email, cloud accounts, laptops, the network and the people who use them.

	#	CHECK	CIS V8.1	NIST CSF 2.0
☐	1	Every device that touches company data is on a list: owner, type, operating system.	1.1	Identify
☐	2	Devices nobody can account for are removed or approved.	1.2	Identify
☐	3	Software in use is listed, and anything no longer supported by its vendor is replaced.	2.1, 2.2, 2.3	Identify
☐	4	AI assistants, browser extensions and cloud storage connected to company accounts are listed and approved.	2.1, 2.3, 15.1	Identify
☐	5	Paid AI plans are checked for whether they train on your data, and staff have a short AI use policy.	3.1	Govern
☐	6	You know where customer and financial data lives, and who can open each folder or app.	3.2, 3.3	Identify
☐	7	Old data and old devices are deleted or wiped on a schedule.	3.4, 3.5	Protect
☐	8	Every user account is on a list with its owner and role.	5.1	Identify
☐	9	Access is granted through a simple written process, and removed the day someone leaves.	6.1, 6.2	Protect
☐	10	Accounts unused for 45 days are disabled.	5.3	Protect
☐	11	Two-factor login is on for email and every cloud app reachable from the internet.	6.3	Protect
☐	12	Two-factor login is on for VPN and remote desktop.	6.4	Protect
☐	13	Admin rights sit on separate admin accounts, held by as few people as possible, with two-factor login.	5.4, 6.5	Protect

	#	CHECK	CIS V8.1	NIST CSF 2.0
☐	14	Passwords are unique and kept in a password manager, not a shared spreadsheet.	5.2	Protect
☐	15	Laptop disks are encrypted, and screens lock on their own.	3.6, 4.3	Protect
☐	16	Operating systems and applications update automatically.	7.3, 7.4	Protect
☐	17	Anti-malware runs on every device and updates itself; USB autorun is off.	10.1, 10.2, 10.3	Protect
☐	18	The device firewall is on for every laptop.	4.5	Protect
☐	19	Browsers and email clients are current, supported versions.	9.1	Protect
☐	20	DNS filtering blocks known malicious sites for office devices.	9.2	Protect
☐	21	SPF, DKIM and DMARC are set for your email domain, so nobody can send mail in your name.	9.5 (beyond IG1)	Protect
☐	22	The router has its default password changed and current firmware; guests use a separate Wi-Fi.	4.2, 4.7, 12.1	Protect
☐	23	IT vendors, hosting and key SaaS providers are on a list with a contact for each.	15.1	Govern
☐	24	Staff are trained to spot phishing, handle data and report a problem, at least once a year.	14.1 to 14.8	Govern
☐	25	One person is named to handle incidents, and everyone knows how to reach them.	17.1, 17.2, 17.3	Respond

Website 7 checks

The site, its hosting, its domain and everything around them.

	#	CHECK	CIS V8.1	NIST CSF 2.0
☐	26	Admin pages are not open to the whole internet, or are protected with two-factor login.	6.3, 6.5	Protect
☐	27	The CMS, plugins and themes are updated, and unsupported ones are removed.	2.2, 7.4	Protect
☐	28	No forgotten test copies, backup archives or config files can be downloaded from the site.	4.1	Protect
☐	29	Logins to the hosting panel, the site admin and the domain registrar are listed and protected with two-factor login.	5.1, 6.5	Protect
☐	30	HTTPS is used on every page and certificates renew automatically.	beyond IG1	Protect
☐	31	DNS records point only to services you use today.	beyond IG1	Identify
☐	32	Site files and database are backed up automatically to storage outside the hosting account.	11.2, 11.4	Protect

Servers and cloud machines 10 checks

VPS, cloud instances and anything with a public address.

	#	CHECK	CIS V8.1	NIST CSF 2.0
☐	33	Open ports seen from the internet match a written list of what should be open, checked from outside.	4.4	Detect
☐	34	The live firewall rules deny by default; the running state is checked, not the config file.	4.4	Protect
☐	35	Logins use keys only; password login and direct root login are off.	4.7, 5.2	Protect
☐	36	Admin access goes only through a VPN or a short list of addresses.	4.6, 6.4	Protect
☐	37	Security updates install automatically.	7.3	Protect
☐	38	Repeated failed logins are blocked, and the block list itself shows it working.	beyond IG1	Detect
☐	39	Default and unused accounts are disabled.	4.7, 5.3	Protect
☐	40	Logs are collected and kept long enough to investigate an incident.	8.1, 8.2, 8.3	Detect
☐	41	A person gets an alert when a new port opens, a new process appears or a backup stops.	beyond IG1	Detect
☐	42	Someone owns checking for vulnerabilities, with a target for how fast fixes go in.	7.1, 7.2	Identify

Apps built with AI coding tools 7 checks

Lovable, Bolt, Cursor, Claude Code and similar.

	#	CHECK	CIS V8.1	NIST CSF 2.0
☐	43	No API keys for AI, payments or email sit in front-end code or anywhere in the git history.	beyond IG1	Protect
☐	44	Database tables have row-level security or locked-down rules; no visitor can read other users' data.	3.3	Protect
☐	45	The server checks permission on every request; changing an ID never shows someone else's records.	beyond IG1	Protect
☐	46	Admin pages require a login, and payment webhooks verify the sender's signature.	beyond IG1	Protect
☐	47	Login, sign-up and AI endpoints have rate limits.	beyond IG1	Protect
☐	48	Dependencies have no known vulnerabilities and are updated regularly.	7.4	Identify
☐	49	AI provider accounts have a spending cap and an alert.	beyond IG1	Govern

Backups and recovery 5 checks

What happens on the worst day.

	#	CHECK	CIS V8.1	NIST CSF 2.0
☐	50	Everything you could not afford to lose is backed up automatically.	11.2	Protect
☐	51	A written recovery instruction sits next to the backups: what to restore, in which order, by whom.	11.1	Recover
☐	52	Backups are protected: encrypted, and not deletable by an ordinary account.	11.3	Protect
☐	53	At least one copy is isolated from the network or held off-site.	11.4	Protect
☐	54	A real restore has been tested in the last three months.	beyond IG1	Recover

Reading your result

Every empty box is a finding. Start with two-factor login, removed access for people who left, and a tested restore: these close the most common ways small businesses get hurt.

Want a second pair of eyes? A cyber security audit checks every item from the outside and the inside, with evidence, and leaves you a fix plan and registers of what you run: klim.expert/services/security/security-audit

Dmytro Klymentiev, klim.expert. Version 2026-11. CIS Controls is a trademark of the Center for Internet Security; safeguard numbers refer to CIS Critical Security Controls v8.1. NIST CSF 2.0 is published by the U.S. National Institute of Standards and Technology. This checklist is not endorsed by either organization.