FOR SMALL BUSINESSES AND THEIR BROKERS

Cyber insurance renewal checklist

A practical list to gather your records before the questionnaire is due. Start at least 60 days out, earlier if you need help from IT.

A short note before you start. This checklist is not legal or insurance advice. It is not an insurance application, and filling it out does not determine coverage, eligibility, premiums, or whether a claim will be paid. ProvenPolicies does not sell, solicit, or negotiate insurance, and does not fill out insurer applications. Use this to gather your own records. Then review the actual questions with your broker or IT provider. If you are unsure, write that down instead of guessing.

60 days out
Find last year's answers, set the renewal date, and start collecting dated records.

30 days out
Fill gaps, ask IT for exports you cannot get yourself, and note anything that changed.

14 days out
Compare this year's picture with last year's answers before you sit down with your broker.

Before you sign
Read every answer against the records you gathered. Do not sign a guess.

01 The renewal basics

- [ ] **Write down the renewal date and who owns the process**
  Name the person at your company who will gather records, and the broker who will receive them.
  Save: renewal date, broker name, and a short internal owner list.

- [ ] **Pull last year's questionnaire, supplements, and policy**
  You need a baseline. If something changed, you will want to see that clearly before anyone answers this year's questions.
  Save: last year's signed application or renewal form, supplements, and the current policy declarations.

- [ ] **List the systems that matter for the questions**
  Email, remote access, backups, laptops, servers, and the main cloud apps that hold company or customer data.
  Save: a one-page inventory with product names and who administers each one.

02 Multi-factor authentication

Questionnaires often ask whether MFA is enforced on email, remote access, and privileged accounts. Enrollment alone may not be the same thing as enforcement.

- [ ] **Confirm MFA on email**
  Check the admin setting that requires a second factor, not just a list of people who turned it on.
  Save: a dated screenshot or export of the enforcement policy, plus any accounts that are excluded and why.

- [ ] **Confirm MFA on remote access and admin accounts**
  Include VPN or other remote tools, and anyone with admin rights in email, Microsoft 365, Google Workspace, or your main line-of-business apps.
  Save: dated settings from each remote tool and a short admin-account list.

- [ ] **Note exceptions in plain language**
  If MFA is not on everywhere the question asks about, write that down. Talk through it with your broker instead of stretching the answer.
  Save: a short exception list with dates and a plan, if you have one.

03 Backups and restore testing

- [ ] **Write down what is backed up, where it lives, and who can delete it**
  Email, files, finance systems, and line-of-business apps often sit in different places. Isolated or offline copies are a common follow-up question.
  Save: a short description of backup products, locations, retention, and who has delete rights.

- [ ] **Get proof of recent successful backup jobs**
  A setting that says backups are on is not the same as a recent successful run.
  Save: dated job logs or a console export that shows recent successful runs.

- [ ] **Find the last test restore, including the date and result**
  If you have not tested a restore recently, say so. Do not treat a successful backup job as proof that you can get the data back.
  Save: a dated note or ticket from the last restore test, including what was restored and whether it worked.

04 Endpoint protection and updates

- [ ] **List computers and whether endpoint protection or EDR is installed**
  Compare the tool's device list with the computers your company actually uses, including laptops that travel.
  Save: a dated device list from the admin console, and a note on who watches alerts.

- [ ] **Show how updates get installed, and when they last ran**
  Know how quickly patches land, who confirms they installed, and whether any machines are behind.
  Save: a dated patch or update report for computers and major servers.

05 Training and people

- [ ] **Gather training completion records**
  Who completed training, when, and what it covered. A calendar invite is not a completion record.
  Save: a dated completion report, or signed attendance records if that is what you use.

- [ ] **Confirm staff know how to report a suspicious email or an incident**
  A short, current instruction is enough. If it is buried in an old handbook, update the date and make sure people can find it.
  Save: the current reporting instructions and the date they were last shared.

06 Incident process

- [ ] **Locate your written incident process and the date it was last reviewed**
  Many questionnaires ask whether a written plan exists. If you have one, make sure it names who does what, and how you reach your broker or insurer after an incident. If you do not have one yet, write that down.
  Save: the current plan or process document, with its date and who approved it.

- [ ] **Write down how you would reach help after hours**
  IT provider, broker, and any breach contacts your insurer has already given you. Keep this in the same folder as the plan.
  Save: a one-page contact list. Do not store passwords or access codes in this folder.

07 Admin access and devices

- [ ] **List who has admin rights, and why**
  Include email, computers, and the main cloud apps. Shared admin logins are a common weak spot.
  Save: a dated admin list for each major system, with personal accounts rather than shared ones if that is how you work.

- [ ] **Confirm laptop and desktop encryption is on**
  BitLocker, FileVault, or the tool you actually use. Check the status, do not assume it from a purchase date.
  Save: a dated encryption status export or screenshot for each computer, including exceptions.

08 Email and domain protections

- [ ] **Check SPF, DKIM, and DMARC for your email domain**
  These come up often because they help stop spoofed email that looks like it came from you.
  Save: a dated screenshot or report of the current records and policy, plus who manages the domain.

09 Vendors and service providers

- [ ] **List outside companies that can access your data or systems**
  IT providers, payroll, tax, document storage, email, backups, and any vendor with a login or a copy of customer information.
  Save: a vendor list with what each one can access and where the contract or terms live.

- [ ] **Note how you check that those vendors still belong on the list**
  You do not need a perfect program. You do need to know who has access and when you last looked.
  Save: the date of the last vendor review and any open follow-ups.

10 Before you answer or sign

- [ ] **Compare this year's records with last year's answers**
  Tools change. People leave. A control that was true last year may not be true now.
  Save: a short change list, including anything you improved and anything that slipped.

- [ ] **Walk the open questions with your broker and IT provider**
  This checklist is only a gathering tool. Your broker can help you understand what the actual form is asking. ProvenPolicies does not fill out that form for you.
  Save: the final set of records you will keep with a copy of whatever is submitted, plus the date.

If you want a place to keep these records, track the renewal date, and come back to them next year, that is what ProvenPolicies is for. It helps you gather and organize documentation. It does not sell insurance or give coverage advice. Learn more at provenpolicies.com.

It does not name every question a carrier may ask. Requirements vary by insurer, policy, industry, and year. Always use the actual questionnaire and your broker's guidance. This checklist is not legal or insurance advice. ProvenPolicies does not sell, solicit, or negotiate insurance. © 2026 ProvenPolicies.