



COMPUTER TIES IT RESOURCE CENTER • CHECKLIST

Vendor & Third-Party Technology Access Checklist

A way to work out who outside your organization can reach your systems and your information, and whether they still should.

FILLABLE PDF

Type into any field, then save or print a copy.

EDITION

Version 1.1 • September 2026

QUESTIONS?

(517) 788-6393 • computer-ties.com

Most organizations have given more outside companies access than they realize. The software supplier who set something up years ago. The accountant with a login. The camera installer who left themselves a way in. The marketing agency that still controls your website.

None of that is unusual, and most of it started for a good reason. The problem is that access is almost never taken away once the reason has gone, and somebody else's security problem can become yours.

This checklist is about knowing who has access, why, and how it ends.

How to use this document

Start with section 1 and simply list everybody. Do not evaluate anything yet. Most organizations are surprised by the length of the list.

Then work through sections 2 to 5 for the ones that matter most: anybody who can reach your money, your customer information, or your systems from outside the building.

A filled-in copy describes who can get into your systems, so store it carefully.

The words you will hear, and what they actually mean

Third-party risk

The risk you inherit from companies you rely on. Their security becomes part of yours the moment you give them a login, whether or not anyone wrote that down.

Supply chain attack

Attacking a supplier in order to reach that supplier's customers. Rather than picking a hundred locks, pick the locksmith.

Standing access and just-in-time access

Standing access is a login that works whenever they like. Just-in-time access is switched on for a job and off afterwards. A key you handed over for good, against one you buzz in each visit.

Business associate agreement (BAA)

Under HIPAA, the written agreement required with a vendor who handles protected health information on your behalf. If you are covered by HIPAA and cannot produce one for a vendor with access, that is a finding waiting to happen.



1 Who Actually Has Access

Fill this in before judging any of it. The list itself is usually the most valuable part of the exercise.

Company	What they do for us	What they can reach	Since	Still needed?

■ Prompts, so you catch the ones people forget

- ☐ Your IT provider, and anybody who worked on your systems before them.
- ☐ The supplier of the main program your business runs on.
- ☐ Your accountant or bookkeeper.
- ☐ Your payroll provider.
- ☐ Whoever built or maintains your website, and whoever holds your domain name.
Losing control of a domain name is unusually painful and unusually common.
- ☐ Your camera, door access, and alarm installers.
- ☐ Copier and printer suppliers, many of which connect remotely for service.
- ☐ Anybody who supports specialist equipment: medical, dental, shop floor, laboratory, point of sale.
- ☐ Marketing agencies, and anyone with access to your social accounts.
- ☐ Cleaners, contractors, and anybody with a key or a door code.
- ☐ Former employees who now work for a supplier.
This one catches people out surprisingly often.



2 The Questions Worth Asking About Each One

Question	Why it matters
Do we know who at that company can reach our systems?	'The vendor has access' usually means several named people do, and their staff change without telling you.
Do they use their own named logins, or a shared one?	A shared login means you can never tell who did what, and it usually never gets changed.
Is two-step sign-in turned on for their access?	Their password is as much of a risk to you as one of your own.
Can they get in whenever they like, or only when we let them?	Access that is switched on for a job and off afterwards is far safer than standing access nobody reviews.
What can they actually see?	Access granted for one narrow purpose often turns out to reach far more than expected.
Do they hold any of our information at their end?	If they do, their security problem becomes your disclosure.
What happens if we stop working with them?	Decide how access ends, and who holds the accounts, before you need to.
Would they tell us if they had a breach?	Many contracts are silent on this, which means the answer is probably no.

3 Before You Give Anybody New Access

- ☐ Agree what they need before granting anything, and grant only that.
It is much easier to add access later than to take it away.
- ☐ Give them their own named login rather than sharing an existing one.
- ☐ Turn on two-step sign-in for their access.
- ☐ Agree how long the access lasts, and put the end date on the calendar.
- ☐ Agree who at their company will be using it, and ask to be told when that changes.
- ☐ Agree what happens to any of your information they hold.
- ☐ Write down who authorized it, and why.
- ☐ Agree that they tell you promptly if they have a security incident.
If it is not written down anywhere, do not assume it will happen.
- ☐ Check whether your own obligations, or your insurer, require anything specific of suppliers with access.

4 The Accounts You Should Own Yourself

The test

If you fell out with this supplier tomorrow, could you still get into it? If the answer is no, the account is in the wrong name. This is the single most common and most expensive vendor problem there is, and it is entirely preventable.

- ☐ Your domain name, and whoever it is registered to.
Registered in your organization's name, with your billing details and an email address you control.
- ☐ Your website hosting and the website itself.
- ☐ Your Microsoft 365 or Google account, including at least one administrator login your organization holds.
- ☐ Your Google Business Profile and other listings.
- ☐ Your social media accounts.
- ☐ The main program your business runs on, and its data.
- ☐ Your camera and door access systems, including the administrator account.
- ☐ Your phone service and phone numbers.
- ☐ Anything a supplier set up using their own email address.
It works fine right up until they stop answering the phone.

5 When the Relationship Ends

- ☐ Their access is switched off on the agreed date, not whenever somebody remembers.
- ☐ Any shared password they knew is changed.
- ☐ Accounts registered in their name are transferred into yours before you part ways.
- ☐ You have a copy of your own information in a format you can actually use.
- ☐ You have the documentation, license keys, and account details needed to keep things running.
- ☐ Their remote access is removed, along with anything they installed to enable it.
- ☐ Keys, fobs, badges, and door codes are returned or canceled.
- ☐ You confirm in writing what they will do with any information they still hold.
- ☐ You record the date access ended, and who checked.



6 Review Record

Supplier	Reviewed on	Access kept, reduced, or removed	By whom

Organization

Completed by

Date

Next review

About this checklist

This is general guidance to help you review outside access. It is not legal or contractual advice, and it does not tell you what your agreements actually say. Organizations covered by HIPAA, CJIS, IRS requirements, PCI DSS, the FTC Safeguards Rule, or defense contracting requirements often have specific obligations about suppliers who handle their information, including written agreements. Confirm what applies to you and involve appropriate legal help.

Not sure who can get into your systems?

Computer Ties can go through the outside access into your environment, tell you what each one can actually reach, and help you close what is no longer needed. We can also make sure the accounts that should be in your name actually are, which is the part that matters most if a relationship ever ends badly.

NEW PROJECTS AND PLANNING

(517) 788-6393

EXISTING CUSTOMER SUPPORT

(517) 905-3168

2903 West Michigan Avenue, Jackson, MI 49202 • computer-ties.com • Serving Jackson since 1990

