FREE RESOURCE · DATA SECURITY STRATEGIST

Data Protection Checklist

Simple checks for the data your business already holds

A checklist and 30–90 day mini plan — not an audit or legal stamp.
About 45–75 minutes.

Andre Brown · andrenbrown.com
Secure · Connect · Optimize

Who this is for

If your business holds customer, employee, or payment data and you want a plain look at how that data is protected, use this form. Mark **Don't know** when you're unsure — that counts as a finding.

1. **Map** what data you have. 2. **Check** controls. 3. **Score** and prioritize. 4. **Commit** to a mini plan.

Section 1 — What data do you have?

A. Types of data

Data type	We have this? (Yes/No)	Examples / notes
Customer or client contact and account info		
Files or documents customers trusted you with		
Employee / HR / payroll		
Payment, banking, or card-related data		
Internal pricing, plans, or private business files		
Health, school, or other tightly regulated data		
Other: _____		

B. Where it lives

Location	In use? (Yes/No)	What data is here?
Microsoft 365 / Google Workspace		
CRM or project tools (HubSpot, Salesforce, and so on)		
Accounting / finance apps		

Location	In use? (Yes/No)	What data is here?
Shared drives, file servers, or Dropbox-style tools		
Email inboxes (including old mail saved on a computer)		
Laptops / desktops with local copies		
Phones / tablets		
Vendor or contractor systems		
Paper or scanned archives		

C. Why this matters

Question	Your answer
If this data leaked, who gets hurt?	
If this data were gone for a week, what stops?	
Is a customer, insurer, or regulator asking about protection?	

Section 2 — Protection checklist

For each row, pick one: **In place · Partial · Missing · Don’t know**

1. Who can get in

Check	Rating	Notes
Real named logins (not shared “team” passwords) for systems with sensitive data		
Only a few people have full admin / owner control		
New people get access on purpose (not by accident)		
Access is removed when someone leaves		
Ex-staff and old vendor accounts checked in the last 90 days		

2. Stronger sign-in

Check	Rating	Notes
Extra login step (MFA / authenticator) on email		
Extra login step on apps that store customer or money data		
Extra login step on remote access / VPN (if you use it)		
Strong unique passwords (or a password manager) for shared team use		

3. Sharing

Check	Rating	Notes
Shared files default to private (not “anyone with the link”)		

Check	Rating	Notes
Public or outside links get reviewed once in a while		
Staff know not to forward sensitive files to personal email		
Customer data isn’t kept in personal cloud accounts by default		

4. Computers and phones

Check	Rating	Notes
You know which work devices hold company data		
Screen lock turns on when devices sit idle		
Device encryption is on where you can turn it on (BitLocker, FileVault, or similar)		
You know what to do if a device is lost or stolen		

5. Backups and restore

Check	Rating	Notes
Important business data is backed up (not only “it’s in email”)		
Backups cover the important places from Section 1		
Someone knows how to ask for a restore		
A restore has been tested in the last 12 months		
Backup isn’t only on the same always-connected drive as the live files		

6. How long you keep data

Check	Rating	Notes
You roughly know how long you keep customer and HR data		
Old data you no longer need can be deleted or archived on purpose		

Check	Rating	Notes
Mailboxes and drives for people who left have a clear owner		

7. Vendors

Check	Rating	Notes
List of main vendors that store or handle your data		
You know who manages each important vendor account		
Contracts or terms for key vendors are easy to find		
When you stop using a vendor, you remove their access and copies when you can		

8. If something goes wrong

Check	Rating	Notes
Named person who leads if email or accounts are taken over		
First steps written down (even half a page): lock it down, reset, notify		
Important contacts handy (IT help, bank, key customers, cyber insurer if any)		
Staff know how to report a suspected problem quickly		

Section 3 — Quick score

Rating	Count
In place	
Partial	
Missing	
Don’t know	
Missing + Don’t know (combined)	

0–4 keep what works · **5–10** pick 3–5 fixes for 30–90 days · **11+** get structured help. “Don’t know” counts as risk until you check.

Section 4 — What to fix first

#	Weak spot (from Section 2)	If this fails, what happens?	First fix this month	Owner	C / H / M
1					
2					
3					
4					
5					

C = Critical (days) · H = High (30 days) · M = Medium (this quarter). Good starts: MFA, remove old access, prove a restore, turn off forgotten public links.

Section 5 — Mini protection plan (30–90 days)

Where you are now

Where you want to be

Three commitments

#	What we'll do	Done by	Owner	Done?
1				☐
2				☐
3				☐

Not in this round

Re-score Section 2 on

Section 6 — Next steps

Do it yourself

- Finish Sections 1–4.
- Complete the three commitments in Section 5.
- If those areas are weak, start with MFA, old access, and one restore test.
- Score yourself again in 90 days.
- Keep this PDF with your IT notes for insurance or customer questions.

When to get help

- Lots of Don't know and no time to dig in

- A customer or insurer wants a clearer story than a self-checklist
- You want a practical plan built and documented for the team
- You've already had an incident or a close call

Want help turning this into a protection plan?

Data Protection Strategies · andrenbrown.com · Start your project