Storing and backing up data

There are many ways to store and back up business data, from laptops and mobile phones to the cloud. Having a long-term plan about how you’ll collect, keep and backup important data goes a long way in keeping things ticking along easily and safely. Here are tips to choose the best storage options for you.

Data worth protecting

This can mean any information you collect, store or use. This might be anything from tax records to a customer information database or secret recipes to employee files.

The larger your business grows, the more thought and effort you’ll need to put into keeping your data organised and safe. Put some solid plans and procedures together sooner rather than later. It will save you time. It will also protect against losing important information if something breaks down or you are hit by a cyber attack.

Important things to consider when backing up your data(external link) — CERT NZ

Protecting business data (/risks-and-operations/it-risk-and-avoiding-scams/protecting-business-data/)


What to do if you’ve been hacked (/risks-and-operations/it-risk-and-avoiding-scams/what-to-do-if-youve-been-hacked/)

Work out your data storage needs

The amount and type of data you need to store will depend on your line of work and how quickly it’s updated. The type of back-up media you use and how often you should back up depends on how quickly you want to restore it after an incident. To find the best storage option, it’s important to know what data you use and how you use it.

Data types

The first step is to list data you have in paper records, stored electronically or on devices used in your business. The second step is to identify what you need to run your business — what you couldn’t do without or find elsewhere if needed. This could include:

- emails
- bills
- invoices
- receipts
- tax records
- employment records
- supplier details
- customer or client information, eg contact details, bank accounts and payment details
- sales records
• documents, reports and other work files
• spreadsheets
• contracts and sales agreements
• photos and images.

Under the Privacy Act, you must do everything you reasonably can to keep information safe. The more sensitive the information, the more security measures you will need to take.

Tax records (/tax-and-accounting/tax-time-tips/keeping-tax-records/)

Employment records (/hiring-and-managing/managing-people-day-to-day/personnel-files-and-record-keeping/)

Any data that contains sensitive information must be handled with care.

Restrict access to any sensitive information - this means both to users and to the internet. Look for services that offer 2FA and make it mandatory for anyone who accesses this information.


Data use

Next, ask yourself who needs access to the data. Whether you share documents with one or two people or collaborate in teams, make sure your storage solution allows the right access at work and offsite. You’re unlikely to need to store most information for more than a couple of years. But some data, eg tax records and employment files, needs to be kept for longer. Don’t store data longer than you need to. It makes managing the data easier.

Restrict administrator-level access to only those who need it — and to have a secure password or passphrase that’s different from others your business uses. Choose a long, strong passphrase, eg lAte23OfDiana’sSandwiches! — and store it in a safe place.

Restrict administrator-level access to only those who need it.

Have a secure password or passphrase that’s different from others your business uses. Choose a long, strong passphrase, eg lAte23OfDiana’sSandwiches! — and store it in a safe place.

Online storage in the cloud

Many businesses use the cloud — the network of servers that host services on the internet — to store, manage and process at least some of their data. Examples include Google Drive, Dropbox and iCloud.

When looking to sign up to a cloud service, it's a good idea to compare what’s on offer. Think about the following:

Access

Benefits: You should be able to access data anywhere and anytime you can get online, including on a smartphone.
But remember, if you can access it anywhere attackers can too. If you have to access sensitive information out of the office, do it on a secure connection — not an open network or public WiFi hotspot. Make sure staff who work from home use a secure wifi network.


Ask about: Can you easily and securely collaborate on documents with colleagues and clients, eg for day-to-day business and projects?

**Security**

**Benefits:** Storing your data in the cloud — rather than relying solely on a hard drive — means you won’t lose access to it if something happens to your hard drive. To keep sensitive data secure on the cloud, be sure to encrypt it, limit access to authorised people and turn on two-factor authentication. Some cloud services encrypt files for you.


Ask about: Data security. Even if you’re no IT expert, you should still feel confident about what you’re getting. Before you sign up, check the contract. What do the terms and conditions say about cyber attacks or loss of data? You can also ask the service provider about their security practices and when they’ll notify you if there’s a breach. If the answers don’t satisfy you, maybe that service isn’t for you.

[Information security management: ISO standards](https://shop.standards.govt.nz/catalog/27002%3A2013%28ISO%7CIEC%29/view) — Standards New Zealand

**Cost**

**Benefits:** Weigh up how much future storage you’ll need. The cloud can be cheaper when it comes to scaling up your needs.

Ask about: There should be a range of prices depending on how much you want to store and service level. Also ask about special offers for signing up. If you can’t negotiate on price, you can still compare prices between services.

**Service**

**Benefits:** Cloud services often offer levels of service that cater for a range of business sizes and budgets. If you don’t need on-call 24-hours-a-day support, the costs should be much lower.

Ask about: If it’s an overseas service with different business hours to New Zealand’s, does this affect response times to queries? If it becomes unavailable, what’s their response time to get you back up and running again? If you hold government data, you may be required to use a New Zealand-based cloud server. The Government Communications Security Bureau has a manual on keeping government information secure.


**Changing providers**

**Benefits:** It’s usually very easy to change services. Notice times will be in your contract.

Ask about: If you want to switch providers, what happens to your data? How easy/secure will it be to transfer it?

**Storage space**

**Benefits:** It’s usually easy to upgrade or purchase more space if you need it.

Ask about: Different storage plans available and any costs to switch.

Also think about

**Reputation:** Check the service’s reputation by doing an online search of its name and words like “security”, “privacy” and “breach”.
Privacy and data protection rules can vary between countries. If your business is concerned about privacy, ask where your data will be stored. You are ultimately responsible for protecting personal information, regardless of whether it’s stored in New Zealand or overseas.

Cloud computing checklist for small business(external link) — Privacy Commissioner

Always encrypt sensitive data — no matter how you decide to store it.

Encryption makes data indecipherable to those who don’t have the key to access it.

Other storage options

These can be used instead of — or in addition to — cloud storage:

**Personal computer:** If you don’t have lots of data, a PC hard drive is an option. Large amounts of data on a PC can dull its performance, but you can boost storage if needed.

**Server:** Unlike a desktop computer, which provides a hard drive and operating system for only one user, a server is a much more powerful device that provides services to many users, eg file access and storage. You’ll need IT help to maintain one. Ask them how often they update them and how they’ll secure them.

**External hard drive:** These offer more storage than a PC, and are relatively cheap and easy to transport — a good option for backing up data and offsite storage. Remember to put encryption on it to prevent it getting stolen.

**USB drive:** Also known as a USB stick or flash drive, they’re small and can store moderate amounts of data — an option for backup copies or for working offsite. Put a password on it so if it gets lost, it’s still protected.

**Disc:** DVDs and CDs can store moderate amounts of data and can be useful as backups to keep offsite.

**Filing cabinets and storage:** If you store paper files with sensitive information, eg customer details and personnel files, make sure you keep them in locked cabinets. Consider a fireproof model for extra protection.

Backing up data

You should regularly make copies of data — known as backing up — in case original data is lost or stolen. It’s also vital for your disaster recovery. If you store data in the cloud, this should be done for you. If not, look at getting software that backs up data automatically, so you don’t need to think about it.

**Tips for backing up**

- **Do it regularly:** If it’s not automated, back up your system at least daily.
- **Secure it:** Protect files with passwords, which should be noted and kept securely at work and offsite.
- **Back up everything:** This includes any device used for your business, eg smartphones, tablets and computers.
- **Keep several copies:** Store copies of backups in different locations — physically and/or in the Cloud — to spread the risk.
- **Test it:** Check your back-up process works by trying to retrieve stored data. When you’re happy it works, set a schedule to test regularly.

Backups for your business(external link) - CERT NZ
Emergency planning (/risks-and-operations/planning-for-the-unexpected-bcp/emergency-planning-for-businesses/)

Test your backups regularly.
You don’t want to need them and find they don’t work or haven’t backed up what you expected.

Smartphones often store or access huge amounts of data.
Make sure to back them up — or set automatic backups — encrypt, and protect them against theft or loss.

Training staff
Storing and backing up data only works if everyone in your business plays their part. Make sure everyone is on the same page about which data to store, and how to do it. It’s worth putting some procedures down in writing.

Make sure you tell staff why storing information is important. Well-managed filing systems make life easier for everyone. If you use online storage services, remember some people will be less technologically savvy than others. Be prepared to give staff support or training if they need it.

It’s also worth helping staff form good online habits, including:

- always signing out of online services
- not saving passwords
- closing browsers after use.

Cyber security awareness for your staff(external link) (https://www.cert.govt.nz/business/guides/policies-and-processes/cyber-security-awareness-for-your-staff/) - CERT NZ

Workplace policies, made easy(external link) (https://wpb.business.govt.nz/workplacepolicybuilder/startscreen/) — Workplace Policy Builder

Avoiding scams and fraud (/risks-and-operations/it-risk-and-avoiding-scams/avoiding-scams-and-fraud/)

Rating form

How helpful did you find this information?

Rate this
- ☐ 1 Star
- ☐ 2 Star
- ☐ 3 Star
- ☐ 4 Star
- ☐ 5 Star

"Rate this" is required

Additional comments

Submit
Loading...

Related content
Making tax time easier

See how

Who will do what in your business?

Learn about the new responsibilities for business owners and operators, plus their staff, visitors and customers.
Read all about it!

Boost your business confidence

(http://build-your-business-confidence/)
Our best tips, tools and visual guides to boost and test your knowledge and skills.
(http://build-your-business-confidence/)
Check it out
(http://build-your-business-confidence/)

Scammers don’t go on holiday

Get your systems in good shape before Christmas so you can rest easy.
Here’s how