

Introduction

In today's digital age, secure data storage and regular backups are essential to reduce the impact of cyber incidents and unexpected business disruptions.

This fact sheet provides practical advice on how small businesses can implement robust storage and backup strategies, ensuring critical information remains safe, accessible, and recoverable in the event of data loss or a cyber incident.

First, it is important to understand what types of data you hold and how you access it. Notably, consider if and how you store:

- Personal information (customer, supplier or employee names and contact details)
- Financial records or payment details
- Identity information (driver licences, passports, or other government documents)
- Sensitive contract and legal information
- Other types of data that you collect when delivering your services

It is important to make sure your data is secured as you may have legal obligations to maintain security standards. Small businesses generally don't fall under the *Privacy Act 1988* (Cth), however, there are some conditions in which a small business may fall under this Act. These include:

- > \$3 Million turnover annually
- Collects health information
- and/or; has contracts with government

If you are unsure whether fall under the *Privacy Act 1988* (Cth), IDCARE suggests getting legal advice. For more information here: [Small business | OAIC](#)

The steps below offer a practical approach in storing your data securely:

1. Create an inventory of information collected and stored by your business

Consider the business purpose for which you are collecting this data, and whether there is any unnecessary information that you don't need to collect.

2. Map where data is stored

Common storage locations include:

- Employee computers and mobile devices
- Local file storage
- Microsoft 365 (Sharepoint, OneDrive, Teams, Outlook)
- External USBs or hard drives

A simple spreadsheet capturing the data type, storage location and relevant internal stakeholders will suffice.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

3. Identify who has access

Review all users who can access business systems and information.

Consider:

- Staff (both former and existing)
- Contractors

Record:

- Who has access
- What level of access (can they edit records or just view them?)
- Whether access is required

Remember, users should only have access to the information necessary to perform their role.

4. Review security controls and consider backups

Avoid using the same or similar passwords across online accounts.

Enable multi-factor authentication on all accounts to ensure there is an extra step of verification to approve login requests.

Audit logged in devices to ensure there are all recognised by the business.

It is also important to make sure there are backups of your data to enable business continuity, as unforeseeable risks are always possible. The potential events that could prevent your data from being accessible include cyberattacks (particularly those which result in file encryption i.e. Ransomware), natural disasters, or hardware failure. Having multiple copies of your data will decrease the likelihood of disruption to your everyday business operations.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Considerations for ongoing data security

- ☐ **Ensure your storage solution is secure:** If you store employee documents in a filing cabinet, make sure it is locked. If you are storing data on a hard drive or USB, ensure it is kept within a locked safe, and where possible, encrypt the drive to prevent any unauthorised access should the drive go missing. If you are using a cloud storage solution (such as Google Drive, OneDrive etc.), make sure the account that is used to access it has multifactor authentication enabled and has a password that is not used in ANY other account.
- ☐ **Implement the 3-2-1 backup rule:** The rule is a simple and effective strategy for protecting your data. It recommends having three copies of your data: the original data stored on your device, plus two backup copies. These copies should be stored on two different types of media, with one backup kept offsite, such as in a secure cloud service.
- ☐ **Access controls:** Consider who in your business needs access to certain information. Implement strict access controls so only authorised personnel can view or modify the data.
- ☐ **Regular reviews of data:** Implement processes to regularly review what data is stored and delete or archive information no longer needed. Your policy should ensure compliance with the "data minimisation" principle, where only the necessary data is kept for the required period. If you need to dispose of paper-based files, consider engaging the services of a data destruction company, for secure file shredding.
- ☐ **Track accountability of data:** Allocating and reviewing types of data and where it is stored is a good way to keep an understanding about what data is stored, and where, within your business. Implementing a timeline of when this data should be reviewed is also recommended. Additionally allocating a dedicated person to review the data will help with audit continuity so that if unusual changes are made, someone who has previously reviewed it may have a better chance of identifying irregularities.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Additional resources

The OAIC provides guidance on how businesses should manage personal information, including recommendations for data retention. They emphasise that data retention policies should:

- ☐ Align with the Australian Privacy Principles (APPs), especially APP 11 (security of personal information) and APP 12 (access to personal information).
- ☐ Consider the [Notifiable Data Breaches \[SH1\]](#) scheme, which outlines the actions to take if a breach impacts data security.
- ☐ **Third-party data handling:** If third-party vendors or services are used to store or manage data (e.g., cloud providers), ensure that they comply with [Australian privacy regulations](#) and your internal policies. Your policy should address how third-party relationships are managed and what contractual safeguards are in place.
- ☐ The Australian Signals Directorate (ASD) has provided some additional information. focused onto [small business use for cloud security](#).

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 170 (Aus)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.