Checklist for storage of documents and records in preparation for disasters

Checklist for not-for-profit organisations

Storing key documents before an emergency is crucial. Lost documents during a disaster can hinder an organisation's response, disrupt operations, and impede recovery.

Safe document storage prevents the worst-case scenario: document destruction leading to breaches of ACNC requirements or other legal record-keeping requirements (such as the requirement to keep tax records). This can jeopardise charity status or result in other legal penalties.

Your organisation should have a robust document management policy, which can be integrated into your business continuity plan.

For more information, see our webpage 'How organisations can manage the storage of documents and records in preparation for disasters'.

Checklist for developing an effective document management policy

Identify essential documents

☐

Create a comprehensive list of the organisation's most important documents. Involve a broad cross-section of the organisation to capture the diverse perspectives of different roles.

These documents may include:

- financial documents such as financial and tax records, and regulatory compliance records (such as for ASIC or the ACNC)
- property and equipment records such as land titles, mortgages, insurance, and vehicle registrations
- governance records such as general and director meeting records, and regulatory compliance records
- contracts with suppliers and employees
- client-related documents (for example, organisations supporting refugees may need to keep visa or immigration documents)

Collate physical copies

☐

Checklist for developing an effective document management policy

Collect essential documents and store them in a plastic sleeve or other protective container for easy access during emergencies. Consider keeping them in an emergency bag or using a safety deposit or PO box.

Given the physical nature of many disasters, store copies of key documents outside the organisation's usual operating area. For multi-branch organisations, consider leaving copies with an interstate branch. If not, consider trusted people or storage solutions interstate.

Create digital copies

☐

Create digital backup copies of important documents using one or more of the methods listed below.

While digitising requires initial effort, it's a worthwhile investment compared to the challenges of recovering damaged or destroyed records after a disaster, which may be impossible in many cases.

Digital storage options include scanning hardcopy documents and saving them electronically:

- in a portable storage device, such as a USB drive, that is kept in an emergency bag or safe deposit box (this allows access even without internet)
- on a mobile app (digital identification apps might store documents like a driver's licenses for directors or committee members, which could be helpful for verification purposes during disasters), or
- in a secure cloud-based platform such as iCloud, Google Drive, Dropbox, or OneDrive (you can access documents from anywhere with internet and download them for offline use). Free options come with limited storage, while paid plans offer more space

Have a backup process

☐

- ensure backups are regularly updated to reflect any changes in your documents
- maintain backups in different locations to mitigate risks

Cloud storage offers geographically distributed backups, while local backups on external hard drives can offer additional security.

Note

- Always choose secure storage options with strong passwords or encryption.
- Store copies outside your regular operating area to protect them from physical disasters.
- Choose storage methods that allow easy access during emergencies, even without internet connectivity.