Public Record Office Victoria

Recordkeeping Policy:
Backup Technologies and Records Management

Version number: 1.0
Issue Date: 15 December 2023
Expiry Date: 15 December 2028

1. Application

The Keeper of Public Records has approved a recordkeeping policy for backup technologies and the records / data they store.[1] Public offices are reminded that records / data held in backups are public records and must be managed accordingly.

The policy contains directives for the following:

- **Backups used only for restoration** in the event of a system failure (or similar) as part of ongoing business continuity or disaster recovery programs are considered to hold copies only of records / data.
    - These copies may be disposed of in accordance with the principle of normal administrative practice (NAP) when no longer required for operational purposes.
- **Backups used to store records / data not held in any other system** are considered to hold official business records / data.
    - These official records / data must be actively managed in accordance with PROV recordkeeping standards for the duration of the retention periods of the records / data held.
    - These official records / data must then be disposed of in accordance with the relevant corresponding retention and disposal authority (RDA) issued by the Keeper of Public Records.

Public offices should apply the terms of this policy in line with the PROV Recordkeeping Standards[2], and the *Value and Risk Policy*[3] to relevant recordkeeping decisions and practices.

[1] Please note that references to records / data refers to records, information, and data and that references to backup technologies or backups includes media, software, and services.
[2] https://prov.vic.gov.au/recordkeeping-government/standards-framework
[3] PROV Recordkeeping Policy: A value and risk-based approach to records management, available via PROV's website https://prov.vic.gov.au/recordkeeping-government/document-library/value-risk-policy

2. Policy

It is Public Record Office Victoria's (PROV) position that:

1. Public offices must not delete records / data from business systems until the records / data are able to be disposed of under a relevant and current retention and disposal authority (RDA).[4]
2. Public offices must ensure that information technology (IT) failures, malicious activity, disasters, and operator mistakes do not cause loss of records/data. If backups are used to achieve the above, then the following applies:
    a. Backups are to be made as part of a regular business continuity or disaster recovery program and managed throughout their lifecycle.
    b. Management is to be in accordance with:
        i. the value of the records/data held by the business system being backed up.[5]
        ii. the impact the loss of the records / data stored will have on business, stakeholders, and the broader community.
    c. The business system managing the backup regime must be protected against threats (such as malicious activity). This includes securing Admin accounts used to manage backups to minimise the impact of malicious activity, such as a ransomware attack encrypting or deleting the records / data held by the business system being backed up.[6]
    d. Backups are to be regularly tested to ensure that the records / data on them can be restored in a manner that enables them to remain usable.
    e. Backup technologies are to be used primarily for the short-term storage of records / data to enable their recovery if lost or corrupted due to:
        i. hardware or software failure.
        ii. user or administrator error.
        iii. malicious activity.
        iv. disaster events.
3. **Backups used for recovery and other purely operational purposes** are to be retained until operational use has ceased, and then may be destroyed in accordance with operational business processes under the principle of normal administrative practice (NAP).
    a. Any records / data held on this form of backup **are considered to be copies only** of business records that may be destroyed under NAP, with the official business records / data held elsewhere on a managed system.[7]
4. Where the official business systems holding records / data are to be replaced, moved offline, mothballed, or decommissioned, contact PROV to discuss appropriate preservation solutions.[8]
5. **If backups are used to provide continuing access to records / data that have been deleted from the business systems, the following must apply:**
    a. Any records / data stored **are considered to be official business records and must be managed in accordance with the PROV Recordkeeping Standards.**[9]
    b. Records / data held in the backup system must be disposed of in accordance with a relevant and current disposal authority. [10]
        i. Records / data must be retained for the duration of their retention periods.

[4] https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas
[5] For more information on valuing records, see *PROS 23/01 Strategic Management Standard* and associated Guideline: https://prov.vic.gov.au/recordkeeping-government/standards-framework
[6] Refer to the Essential Eight regarding backup technologies and cybersecurity: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight
[7] https://prov.vic.gov.au/recordkeeping-government/a-z-topics/normal-administrative-practice-nap
[8] Contact us via our enquiry form here: https://prov.altarama.com/reft100.aspx?key=Agency
[9] https://prov.vic.gov.au/recordkeeping-government/standards-framework
[10] https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas

ii. Records / data must not be deleted from backup systems or software until they are able to be disposed of in accordance with a relevant and current retention and disposal authority.
iii. Deletion of records / data without appropriate authorisation is an offense under the *Public Records Act 1973.*[11]
iv. Records / data must remain useable, readable, and accessible for the duration of their retention periods regardless of what system they are held within (including backups).

c. Long term access to the records / data held only in backup systems must be provided where needed and in a manner that:
i. ensures the records / data remain identifiable, discoverable, retrievable, and usable by authorised people until their minimum required retention period has expired.[12]
ii. ensures the ongoing viability of the records / data held on the backup for the duration of their retention periods as part of an ongoing digital preservation program.
iii. collects and keeps sufficient information/metadata about the records / data to enable effective and efficient recovery action to be taken if necessary.[13] High value data/ records require sufficient information/metadata to enable data/record specific identification, extraction, and retrieval in a usable condition as needed.

d. Systems, software, and other associated technologies used to provide long term access to records or data no longer held within active business systems must also be retained (along with the records / data) to ensure continued accessibility and readability.
i. This includes storage of and/or continued access to the application software required to interpret the stored records / data and the backup software/system used to create the backup.
ii. The technologies / software cannot be destroyed or otherwise disposed of until the retention periods of all records and data that require them have passed.

6. Individual media, such as tape or other physical artefacts used to hold the backup, are only to be used if the quantity of data makes other storage uneconomic and must be in accordance with a management regime that ensures:
a. media is not lost.
b. the condition of the media is tracked.
c. the data, information and/or records are copied off the media before the media deteriorates or the technology becomes obsolete.
d. records / data stored on the media are in appropriate long-term preservation formats.[14]

[11] https://www.legislation.vic.gov.au/in-force/acts/public-records-act-1973
[12] If the method of backups used cannot enable this clause to be met, then copies only of records can be stored using that method. Official records will need to be stored using other methods that can enable this clause to be met.
[13] Sufficient metadata or information should be determined by the agency in accordance with *PROS 19/05 Create, Capture and Control Standard* and associated specifications. https://prov.vic.gov.au/recordkeeping-government/standards-framework
[14] Refer to *PROS 19/05 S3 Long Term Sustainable Formats Specification*: https://prov.vic.gov.au/recordkeeping-government/standards-framework

3. Background

PROV developed this policy to address the use of backup technologies to store data, information, and records.

Backups are used for two purposes:

1. to guard against hardware/software failure or operator error as part of disaster records / business continuity programs.
2. to archive data from business applications running on a server, which is not recommended as it places the data / records at risk and should only occur when absolutely essential. Where it occurs, the data / records stored must be managed in accordance with the recordkeeping Standards issued by the Keeper of Public Records. Records / data must remain identifiable, locatable, retrievable, and useable for the duration of their retention periods.

Disposal

Backups used to guard against hardware/software failure or operator error need only be kept for a short period, and the retention duration is a technical decision. Records / data held on such systems are considered to be copies only and may be disposed of under NAP[15] once operational use has ended.

Backups used to archive[16] records / data in the business applications running on the server occur as a result of agency staff members deleting data from the business application and relying on the backups to retrieve the data if it is subsequently required. They are clearly holding records subject to a retention and disposal authority (RDA) and disposal of the backup needs authorisation. Disposal of the backup is now a recordkeeping decision and not a technical one.

Risk

Backup is effective at short term recovery.

Archiving is about long-term access and requires understanding the value of records / data held, as well as their management requirements.

This conflict in time frames means that there is significant risks involved when using backup technology to archive data. For example, there is a major risks that the data will not be able to be recovered as it requires both the backup software and the original application in order to extract meaning from the backed-up records / data.

Technologies used for backups have an impact on a range of factors, including:

- the amount of records / data that can be stored.
- the cost of storage (for example, cloud storage is likely to be more expensive than using media such as tape to store the backups).
- the ability to identify, locate, retrieve, read, and use records / data within an appropriate timeframe.
- arrangements regarding where the records / data are kept, responsibilities and services in relation to them from the perspectives of both the organisation and the service provider, and other contextual arrangements.

Risks from using backup technologies to store records / data without managing them appropriately include:

- the loss of records / data through the overwriting of older records / data as new backups are created, the corruption and degradation of backups held over time, and incompatibility issues as software and other applications evolve over time and may no longer work on older records / data.
- inefficient record / data retrieval as accessing specific records / data from a backup can be slow and cumbersome, especially if they are stored in complex backup formats.
- increased storage costs as backup technology is often designed for redundancy and quick recovery resulting in high risk of duplication and higher storage costs than archival solutions.

[15] https://prov.vic.gov.au/recordkeeping-government/a-z-topics/normal-administrative-practice-nap

[16] Please note that 'archive' in this policy refers to the long-term preservation of records / data complete with context and in a readable, useable, discoverable and accessible format.

- not meeting compliance requirements as records / data are subject to legislative and regulatory requirements including specific retention periods, privacy and data protection requirements, encryption requirements, audit trail requirements. This includes managing records / data over their lifecycle. Backup technologies are generally not equipped to address these well. They also expose the records / data to increased risk of cyber security breaches.
- backup systems may not offer robust search and indexing capabilities, making it difficult and expensive to quickly locate high value or high-risk records / data.

Records / data must be managed in accordance with the PROV Recordkeeping Standards, including the relevant retention and disposal authorities, regardless of where they are stored.