Disaster Recovery Planning for Physical Records

Purpose

In a disaster, the loss of records can cripple business activities. The purpose of this advice is to guide ACT Government agencies in developing an effective disaster recovery plan for any physical records they rely on. This avoids potential risks, minimises disruption, ensures operational continuity, and safeguards valuable assets in the event of a disaster.

This advice relates specifically to disaster recovery planning for physical records. It does not cover cyber security risks and other threats to digital records. Cyber security incidents must be reported to ICT Service Desk as soon as possible. Call 620 79000 and press 1 for ICT. In the event of a disaster affecting a Whole of Government EDRMS, email Digital Records Strategy and Services DigitalRecordsHelpdesk@act.gov.au.

What is a disaster?

In this advice, we refer to a disaster as an event that causes significant damage, loss or harm to an agency's physical records, their management, or the recordkeeping systems that are used to administer them.

Potential threats can be from natural or human causes, and can include flood, fire and smoke, earthquake, pandemic, pests, storms, temperature and humidity, mould, criminal action, human error, power loss, leaks, or building damage. These threats could impact physical records sitting on a desk or a car seat, or stored in a file room or a warehouse.

Which agencies need a disaster recovery plan for physical records?

A disaster recovery plan is essential for any agency that holds physical records. Agencies must take steps to protect physical records from potential threats and include disaster management as part of organisation-wide business continuity plans. A disaster plan is not required for records stored with the Territory Records Office. However, agencies should consider the impact of a disaster involving those records in their business continuity planning.

If agencies holding physical records do not already have a disaster recovery plan in place, it is important to start planning immediately. Early planning for a disaster ensures readiness and helps minimise disruption and unnecessary costs. Preparedness is key to addressing issues promptly and efficiently, which ultimately saves time and resources, and can prevent permanent loss of affected records.

Before a disaster: Develop a disaster recovery plan

1. Identify risks and mitigation strategies.
    a. Conduct a risk assessment to identify potential threats and create strategies to minimise these risks.
    b. For physical records in third-party storage, review the vendor service level agreement to understand expectations for both service provider and customer.

2. Identify critical records and prioritise their recovery.
    a. Use the TRO advice on Vital Records to identify records which are most critical to the operation of the agency.
    b. Create a list of Vital Records and their locations.
    c. Create an action plan to ensure Vital Records are prioritised during disaster recovery efforts. This should form part of the agency Records Management Program.
3. Assess records storage locations and vulnerable areas of the agency.
    a. Assess locations and teams within the agency to identify vulnerabilities and potential improvements. This could include storage locations, facilities, equipment, resources and staffing arrangements.
    b. Where possible, move records out of vulnerable locations as part of mitigation and prevention efforts.
    c. The TRO Guideline on the Protect Principle requires agencies to store records in endorsed locations. The knowledge of where records are located will assist in disaster planning and response.
4. Develop a preventative plan.
    a. Preventative strategies include pest control, maintenance of storage areas, checks of disaster supplies, and monitoring and control measures for temperature and humidity levels.
    b. Schedule regular checks over the course of a year. A Disaster Preparedness Calendar can assist with planning.
    c. Other important preventative measures include ensuring that records are kept in boxes on shelves and not stored on the floor.
    d. Consult with Work Health and Safety experts in identifying and assessing workplace hazards to ensure the agency complies with health and safety regulations and mitigates these risks.
    e. Ensure disaster recovery equipment is available and easily deployed. A designated wheelie bin can provide a useful disaster recovery kit.
5. Assign roles and responsibilities.
    a. Develop a register of key staff to ensure that there are enough people to respond during an emergency.
    b. Ensure there is enough flexibility to allow for some staff being unavailable, for example if a wide-scale disaster is affecting them at home.
6. Identify stakeholders.
    a. This could include employees, management, ACT Insurance Authority, Territory Records Office, WorkSafe ACT, and the ACT Emergency Services Agency.
7. Develop Standard Operating Procedures (SOPs).
    a. Create SOPs for different disaster scenarios, eg water damage, fire.
8. Compile a Disaster Recovery Manual.
    a. It should be straightforward, easy to use in an emergency, and should include:
        i. Disaster response roles and contact information
        ii. Emergency contacts details for essential services
        iii. List of service providers to assist
        iv. Vital records list
        v. Location of disaster recovery supplies
        vi. SOPs.

    b. Ensure both hard-copy and digital manuals are available in appropriate locations.
9. Promote the plan and conduct training.
    a. Ensure all relevant staff are aware of the plan.
    b. Conduct training sessions for new staff and regular refresher sessions for all staff. For staff with particular responsibilities, this could include recovery drills and simulations to ensure they are confident in handling different scenarios.
    c. Ensure that staff understand and use the agency's endorsed locations for records storage.
    d. Evaluate staff knowledge and skills to identify additional training needs in disaster preparedness.
10. Ensure the plan remains current.
    a. Conduct regular reviews of the disaster plan.
    b. Review the plan before periods of staff absence (e.g. Christmas shutdown), and high-risk periods for extreme weather events.

During a disaster: How to respond

1. Survey the scene to ensure it is safe to respond.
2. Assess the overall situation to understand the scope of the disaster.
3. Stabilise the environment to prevent further damage, such as securing the area, controlling leaks, or setting up temporary barriers.
4. Gather equipment and resources needed for the recovery. This includes tools to recover damaged records and to prevent further damage, and personal protective equipment.
5. Record and evaluate the damage. Take photographs and collect any other relevant information to evaluate the impact and prioritise recovery of vital records.
6. Ensure a coordinated response by keeping stakeholders informed about the situation.
7. Notify the Territory Records Office if any records are damaged or destroyed. TRO can provide advice on specific actions for the event.
8. Implement disaster SOPs.

After a disaster: Review and assess what happened

1. Review and evaluate the recovery process to identify what worked well and what could be improved. Include feedback from those involved to get different perspectives.
2. Document lessons learned during the disaster and recovery process, including successes, challenges and unexpected issues.
3. Assess the costs associated with damage and recovery, and look at ongoing financial implications. This includes identifying gaps and ensuring adequate resources are allocated for effective recovery.
4. Prepare a report on the recovery process. This can be a useful case study to assist in the development and improvement of disaster recovery planning.
5. Use the post-disaster analysis to update and improve the disaster recovery plan for future incidents.

Useful References:

Territory Records Office website for Standards, Guidelines and Advices

Territory Records Office Extranet for information and resources for ACT Government agencies

WorkSafe ACT

ACT Emergency Services Agency – Preparing for Emergencies

Australian Capital Territory Insurance Authority

Australian Institute for the Conservation of Cultural Materials - Disaster

Blue Shield Australia

CONTACT US

Territory Records Office | www.territoryrecords.act.gov.au| TRO@act.gov.au