Disaster Preparedness Bulletin 2026

Cayman Islands National Archive
Cayman Islands Government

Safeguarding Records in Offsite Storage Areas

As the 2026 Hurricane Season has begun, many of us should likewise be preparing our workplaces and homes with continuity plans and emergency supplies for potential storms. One area that may be overlooked is the protection of records stored in offsite locations, i.e. warehouses or storage containers.

Offsite storage is often used for inactive records and to relieve office space constraints, but these environments can be extremely vulnerable if not properly maintained and monitored.

Heat, humidity, flooding, leaks, pests, mould, and poor ventilation can quickly damage records and compromise important government information.

Public agencies should monitor and manage any offsite storage areas to ensure the records remain secure, accessible, and protected at all times, but especially throughout hurricane season.

Records should remain secure, accessible, and protected throughout the year.

Simple preparedness measures can make a significant difference

Routine inspections and simple preventive measures can significantly reduce the risk of damage to records stored in offsite locations during hurricane season.

Protecting records today helps preserve continuity, accountability, and resilience for tomorrow.

Offsite Storage Quick Check

- Records stored off the floor.
- No leaks or rust visible.
- Shelving secure and stable.
- Storage areas inspected regularly.
- All records are listed.

Cayman Islands
National Archive
Cayman Islands Government

Legal Requirement

Under section 6(2) of the National Archive and Public Records Act (2026 Revision),"the most senior officer in every public agency [is responsible] to ensure that public records...are maintained in good order and condition". Effective records and information management (RIM) supports accountability, transparency, and continuity of government operations.

What Does This Mean for Senior Officers?

The responsibility extends beyond the physical storage of records, and senior officers should ensure that:

- Records are properly created, maintained, and protected.
- Appropriate security controls are in place.
- Records storage areas meet National Archive standards.
- Vital records can be recovered during emergencies.
- Staff understand and follow RIM policies and procedures.
- Regular reviews are conducted to identify and address risks.

Good records and information management is a leadership responsibility—not just an administrative function.

Consequences of Poor Records Management

- Failure to maintain records in good order and condition can result in:
- Loss of evidence supporting government decisions and actions.
- Reduced accountability and transparency.
- Operational disruption during emergencies.
- Increased legal, financial, and reputational risk.
- Inability to meet statutory and regulatory obligations.

RIM Continuity Check

- Records security and environmental protection.
- Identification and prioritisation of vital records.
- Approved Business Continuity Plan.
- Staff awareness and compliance.
- Recent self-assessment completed

RIM Spotlight

Records and information management is not only compliance — it is about protecting the information assets that enables government to serve the public, make informed decisions, and deliver on obligations.

Cayman Islands
National Archive
Cayman Islands Government

Business Continuity for Recordkeeping

Offsite storage in tropical climates can present significant environmental, operational, and regulatory risks. In the Cayman Islands, these risks are heightened by high humidity, hurricane exposure, salt corrosion, flooding, and underlying infrastructure vulnerabilities, which can threaten the integrity and accessibility of records.

Despite these challenges, risk can be effectively reduced through a combination of mitigation strategies. Climate-controlled facilities, robust disaster recovery planning, backup sites in different locations, and digitisation initiatives all play important roles in strengthening the protection of critical information assets.

For public agencies, offsite storage should be treated as a core element of Enterprise Risk Management and within their Business Continuity Plan (BCP), rather than a ad-hoc operational function. A BCP is essential to ensure that vital records remain protected, accessible, and recoverable during emergencies or disruptions.

BCP should align with the Cayman Islands National Disaster Management Plan (2025) and address both physical and electronic records. It must account for hazards including hurricanes, flooding, fire, cyberattacks, and power outages, while prioritizing the

protection of personnel, safeguarding of records, continuity of critical services, and preservation of legal and financial accountability.

The plan should also address the restoration of access to essential information within defined recovery timeframes, and support modern resilience tools such as the Continuity2 Meridian platform for automation of business continuity, risk management, and disaster recovery processes. Regular testing, annual reviews, and maintenance of a vital records inventory are also necessary to ensure ongoing readiness and compliance with national disaster management and public records obligations.

If records are not recoverable, continuity may not be possible.

Protecting Your Paper Records

- Identify and map all vital records, including floor plan locations.
- Prioritise records once identified.
- Log all items before off-site transfer.
- Store in waterproof containers or fire-resistant cabinets.
- Do not leave documents uncovered overnight.
- Keep records off the floor and away from windows (max 3 boxes high).

Cayman Islands
National Archive
Cayman Islands Government

Guideline 12 Notification of Damaged Records

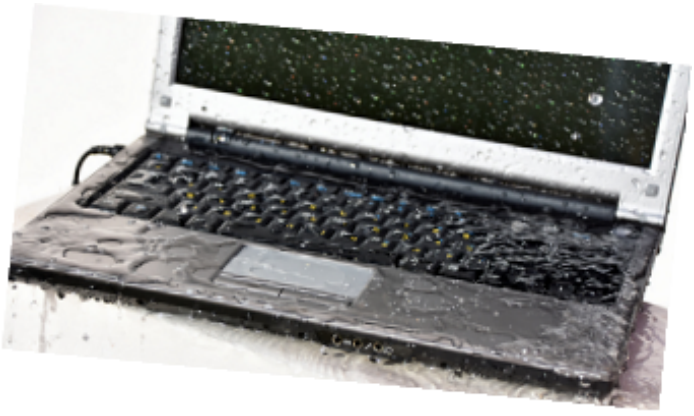
The National Archive's Guideline 12 requires "public agencies to notify [CINA] of any substantial damage from natural or manmade disasters to physical public records." Government records are information assets that support accountability, governance, legal evidence and decision-making.

Public agencies should continuously monitor all storage areas to ensure records are accessible for as long as they are required. Unexpected disasters can occur, so records protection measures should be included in each public agency's BCP.

Agencies must document substantial damage to their physical records to either undertake remediation measures, or to ultimately pursue CINA's authorised destruction protocols for records which cannot be recovered.

Upon discovery of damaged records, time is of the essence to stabilise or prevent further issues. Report damage immediately in writing to the National Archive, using the Damaged Physical Records Notification Form, with photos and supporting evidence.

Agencies should permanently retain a copy of the Damaged Physical Records Notification Form for their official recordkeeping system.



Records Storage Quick Tips

- Avoid storing records on top shelves
- Pack files vertically (spine down) in archival boxes — don't lay flat or overpack (leave 1" space)
- Seal boxes securely and wrap in polythene/plastic sheeting
- Follow fire precautions and ensure staff awareness of hazards and equipment
- Keep aisles, passageways, and exits clear at all times

Stabilisation and Recovery of Electronic Records

Should a disaster impact your facility, consult with first responders, and do not enter your facility until you have received permission to do so. Serious electrical, chemical, and other hazards may be present even in areas that look perfectly safe. If first responders advise destroying your damaged electronic or paper records, assure them that you must first contact the National Archive and your IT service providers, who may have information on how to salvage these materials.

Upon access to your facility, begin identifying electronic storage media affected by the disaster. The sooner you can salvage the media, the greater your chances of recovering the data. Ideally, your salvage efforts should begin no later than 48 hours after the disaster. However, if barred from accessing your facility for a week or more, some of your data may still be recoverable.

The first 48 hours are critical—swift action significantly increases the likelihood of successful data recovery.

Cayman Islands
National Archive
Cayman Islands Government

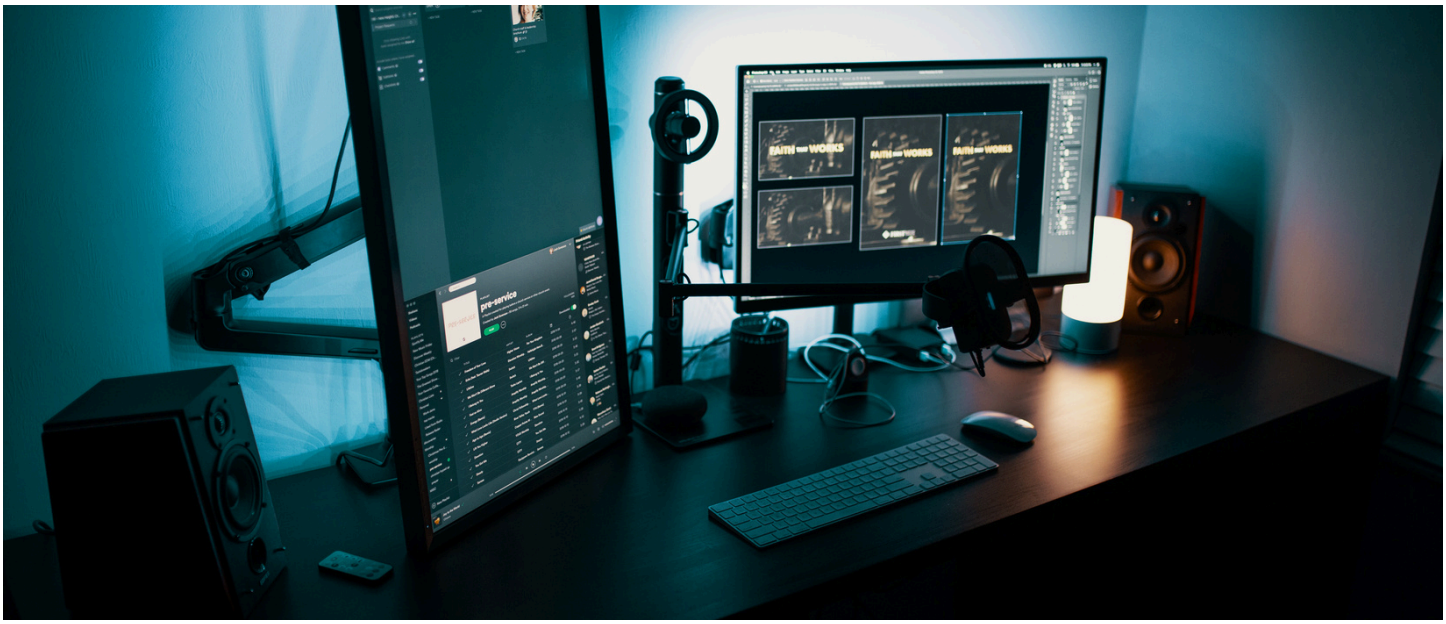
Protecting Electronic Media

To reduce the risk of damage to electronic media during disasters, agencies should undertake the following preparedness measures:

1. Back Up Data – Regularly back up critical information and confirm with CSD that automated backups are enabled and functioning as intended.
2. Use Protective Storage – Store external hard drives, and other media in waterproof, fireproof, and anti-static containers.
3. Maintain Proper Environmental Conditions – Keep media in climate-controlled environments and away from direct sunlight, heat, and excessive humidity.
4. Store Media Safely – Place media in elevated, secure locations and, where possible, maintain copies at a secondary site that is not exposed to the same risks.
5. Protect Against Power Surges – Use surge protectors and UPS systems, and disconnect equipment during severe storms when safe to do so.
6. Conduct Regular Maintenance – Periodically test backups to ensure data can be restored and keep software updated to address security and compatibility issues.
7. Maintain a Business Continuity Plan – Ensure plans include procedures for protecting and recovering electronic media during emergencies.
8. Keep Emergency Contacts and Conduct Drills – Maintain current contact information and periodically test response procedures through exercises and drills.
9. Promote Education and Awareness – Train staff in basic electronic media protection practices and keep them informed of local disaster risks.

By implementing these steps, agencies can significantly reduce the risk of damage to their electronic media from disasters. Regular backups, proper storage, and a well thought-out Business Continuity Plan are crucial components of effective disaster preparedness.

Cayman Islands National Archive
Cayman Islands Government



General Guidelines for Recovering Electronic Media

Protecting electronic media is a critical part of business continuity and disaster recovery. The following guidance provides practical steps for safely handling damaged media and improving the likelihood of data recovery.

Before You Begin

Safety First

- Wear gloves and a mask if required.
- The area should be free from hazards such as standing water, fire, or exposed electrical wiring.
- Never attempt to power on damaged electronic devices.
- Handle damaged media carefully to prevent further harm.

Common Types of Damage

Water Damage

- Remove the device from water immediately.
- Do not shake, open, or disassemble.
- Air dry in a cool, ventilated area.
- Use silica gel packets to absorb moisture.
- Contact a data recovery specialist as soon as possible.

Fire Damage

- Allow the device to cool naturally.
- Gently remove soot using a soft brush or canned air.
- Do not use liquids or attempt to power on the device.
- Seek professional assessment and recovery assistance.

Helpful Tip:
Document the condition of the media, actions taken, and recovery contacts for future reference.

Environmental & Physical Damage

Physical Damage

- Minimise handling.
- Store in an anti-static bag or clean, dry cloth.
- Contact a professional recovery service immediately.

Mould or Dust Damage

- Remove dust gently with a soft brush or cloth.
- Do not attempt to clean mould yourself.
- Store media in a cool, dry environment.
- Seek professional assistance for significant contamination.

When to Call the Experts

Contact a professional data recovery service immediately if:

- The damage is extensive.
- The information is critical.
- Recovery requires specialist equipment or expertise.

Cayman Islands
National Archive
Cayman Islands Government

The National Archive and Public Records Act (2026 Revision) requires public agencies to maintain records in good order and condition. The below assessment tool should help to measure agency compliance with the National Archive's Creation and Maintenance Standard (S1), identify areas for improvement, and strengthen records preservation practices. Questions? Contact cina@gov.ky.

Section	Requirements S1	Questions	Response	Suggested Remedial Response
7	Temperature, RH and Light: Avoid high natural and/or artificial light exposure; store in stable environmental conditions: temp 60° – 80° F and RH 30 – 60%.	Are records subjected to direct light? Are temperatures and relative humidity within acceptable ranges?	☐ Yes ☐ No ☐ N/A ☐ Unsure	• Move records away from direct light. • Check and maintain A/C systems. • Consider using a humidifier.
8(2)	Pests : Silverfish and mice can do considerable damage and infestation can spread easily.	Are there signs of rodents, silverfish or other pests?	☐ Yes ☐ No ☐ N/A ☐ Unsure	• Regular inspection of records for signs of deterioration from pest and mould must be carried out.
8(2)	Mould: High humidity, water leaks, and poor airflow can cause mould growth; increased health risks & damaged records.	Is the location damp or mouldy? Is there growth on papers?	☐ Yes ☐ No ☐ N/A ☐ Unsure	• For suspected mould growth, contact the Department of Environmental Health for an assessment, and the National Archive for further advice.
8	Storage: Storing records on the floor puts them at risk of flooding or water build-up.	Are records stored on the floor?	☐ Yes ☐ No ☐ N/A ☐ Unsure	• Use shelving units to store boxes at least 4 inches off the floor. • Do not stack more than 4 boxes; lower ones can get crushed.
7(5) 8	Security of the location: Records should not be kept in securely regulated areas.	Is the location secured from unauthorised entry and protected from potential theft?	☐ Yes ☐ No ☐ N/A ☐ Unsure	• Restrict and secure access to storage areas; monitor regularly. • Limit access to authorised staff or use locked cabinets.
8	Fire and water: Protect storage facilities from fire and water hazards; conduct regular inspections.	Are records near water pipes, sinks; any signs of leaks? Are records near electrical outlets?	☐ Yes ☐ No ☐ N/A ☐ Unsure	• Consider relocating records. • Repair leaks and electrical outlets. • Install fire detection systems, including fire extinguishers.
7(3) 8(1)	Dedicated record storage areas: Eating, drinking, and smoking must not be permitted in storage areas.	Is there evidence of eating and drinking in record storage areas?	☐ Yes ☐ No ☐ N/A ☐ Unsure	• Clean area and ensure that all staff are aware that no food or drinks should be consumed or even stored in these areas.

Cayman Islands National Archive
Cayman Islands Government

Checklist for Business Continuity Plans

☐ Risk assessment - Identify potential risks and their effect on records and information management systems, and then outline the mediation steps and monitoring processes.
If a disaster occurred, how long could the agency function with available staff until records and recordkeeping systems are back online?

☐ Pre-disaster planning - In your plan, outline the duties/tasks of those responsible for records disaster mitigation and have specific recovery/remediation procedures for dealing with the identified disasters.

- Has adequate storage and security of the records been identified?

☐ Communication - Identify who should be informed in the event of a records disaster and how information will be exchanged. Include instructions on the means of interacting with your stakeholders (e.g. staff, clients and vendors).

- Has your agency's team been briefed? Plan the recovery approach and assign tasks.

☐ Disaster co-ordination - Compile a contact list of external emergency service agencies including the National Archive, the Department of Environmental Health, NEOC, and Hazard Management Cayman Islands.

- Identify the external services/vendors required for normal business operations.

☐ Disaster response - Activate the plan, with priority given to the recovery of vital records and critical data (including lists of records and their locations). Procedures should be in place for handling damaged materials, including the required resources (e.g. staff, alternate locations, equipment, etc.).

- Secure affected areas and assess any damage to records, particularly vital records. Endeavour to collect evidence of damage as quickly as possible with photos and/or written notes/reports. Submit all documentation, along with a Damaged Physical Records Notification Form to the National Archive.

☐ Recovery - Undertake and coordinate the activities for record recovery/remediation, and establish procedures for handling records after a disaster.

- Do not dispose of damaged records as they may be salvageable.
- No public records can be destroyed without a Cabinet-approved disposal schedule and in accordance with the National's Archvie's documented destruciton process.

☐ Post recovery - Review and update the plan.

- What worked and what can be improved.

Effective records and information management isn't just good practice — it's essential for business continuity and resilience. Take a moment today to review your records practices — how you create, store, access, and dispose of information.

Strengthening these practices isn't just good governance — it's an investment in continuity, resilience, and long-term success.

Contact the National Archive at cina_rim@gov.ky for more information.