

Technology Disaster Recovery Playbook

ROBIN HASTINGS / LIBRARY LEADERSHIP

Keep essential services useful. Know what recovery will take.

A practical starting point for library directors, service managers, boards, and technology partners, especially where a small staff carries several responsibilities.

Start with the situation you have

An incident is happening: turn to page 2, name a lead, and use the checklist. Preparing before an incident: begin with one essential service on page 5. Working with a provider: take pages 6 and 7 to the conversation.

This playbook connects service decisions with technical recovery. Adapt the templates with your technology provider and local authorities before adopting them.

Inside

- 2 / First 24 hours
- 3 / Classify the incident and assign authority
- 4 / Assess recovery maturity
- 5 / Set service priorities and recovery targets
- 6 / Choose and test backup arrangements
- 7 / Make vendor dependencies visible
- 8 / Communicate what people need to know
- 9 / Practice three realistic scenarios
- 10 / Spend where it closes a demonstrated gap
- 11 / Record recovery and the next improvement
- 12 / Sources and scope

October 19, 2026

Complete local contacts, authority, and service targets before operational use. Printable worksheets; fields are not electronically fillable.

The first 24 hours

Suggested sequence, not a promise of recovery within a day. Act sooner when risk requires it. Assign each action to a person and record time, result, and the next decision.

Immediately: protect people and limit harm

- [] For fire, water, electrical hazards, or threats to people, follow the emergency plan and contact emergency services. Do not enter unsafe spaces to retrieve equipment.
- [] Name the incident lead and alternate. Record discovery time, affected services, observed symptoms, and what is still unknown.
- [] For suspected ransomware, have qualified responders coordinate isolation of affected systems and use a separate, trusted communication channel. Avoid improvised wiping or rebuilding that could destroy evidence. [1]

First hour: establish control

- [] Contact the technical provider using an independently verified number. If ordinary email may be compromised, use the agreed alternate channel.
- [] Open an incident log. Keep observations separate from assumptions. Preserve messages, timestamps, and technical evidence under responder direction.
- [] Decide which services can continue safely. Pause workflows that depend on uncertain data or unsafe systems. Use only approved fallback procedures.

Hours 1-4: coordinate the response

- [] Assign the service lead, technical lead, spokesperson, and recorder. Contact the governing authority, insurer, or other response partners as applicable to the local plan.
- [] Publish a factual service update and a time for the next update. Have the designated adviser determine applicable notification duties; do not guess deadlines.
- [] Identify clean recovery options, missing dependencies, and the most urgent service needs. Keep recovery media separated from affected systems.

Hours 4-24: sustain and reassess

- [] Schedule staff relief, vendor check-ins, and public updates. Review service impacts and unresolved safety or privacy concerns.
- [] Authorize a controlled recovery test when responders consider it safe. Record observed restoration time and data age; obtain service-owner acceptance before reopening.

If recovery takes longer: repeat status checks, maintain the log, and communicate the next decision time. A vendor estimate is not a confirmed reopening time.

Classify the incident

Use impact and uncertainty to choose a response. These proposed levels are local planning aids, not a NIST or CISA rating system. Reassess whenever new evidence changes the picture.

1 / Limited disruption

Example: one public printer fails, with no indication of a security incident. The service owner coordinates routine support and a workaround. Escalate if the problem spreads, sensitive information is involved, or an essential service target will be missed.

2 / Significant service interruption

Example: internet access or the hosted catalog is unavailable across the library. Activate the incident lead, coordinate vendors, and maintain service-specific updates. Escalate if safe fallback fails or the cause suggests compromise.

3 / Major incident or suspected compromise

Example: a ransom message, suspected unauthorized access to patron records, widespread system failure, or building damage. Activate leadership and qualified responders promptly. Do not wait for proof of data theft before escalating a credible security concern.

Write down who can decide

Incident lead: coordinates priorities and escalation.

Technical lead: directs investigation, containment, and recovery.

Service owner: validates whether staff and patrons can use the service.

Spokesperson: approves and distributes consistent updates.

Recorder: maintains decisions, actions, and handoffs.

In a small library, one person may fill several roles. Each critical role still needs an alternate and a way to reach them when normal systems are unavailable.

Lead and alternate / contact location:

Who may pause or reopen services:

Emergency spending authority / limit / alternate:

Planning basis: NIST treats incident response as part of ongoing cybersecurity risk management, not an activity that begins only after an attack. [2]

Assess recovery maturity

Rate one service at a time. This is a proposed evidence-based conversation guide, not a certification, audit score, or prediction of how fast recovery will happen.

1 / Assumed

Someone believes backups exist or that the vendor handles recovery. The library cannot locate a current test record. Next step: identify the service owner, provider, and data that must be recovered.

2 / Documented

Roles, contacts, targets, dependencies, and fallback steps are written down and accessible during an outage. Next step: ask the alternate to find the plan and walk through it without help.

3 / Demonstrated

A controlled test has restored a representative service. Staff have checked the result, and the record shows elapsed time, data age, and unresolved limitations. Next step: close the most consequential failed dependency.

4 / Maintained

The library repeats exercises and reviews after significant changes, tracks repairs, and has alternates who can carry out their roles. Next step: test a different failure, such as loss of the usual administrator or identity provider.

Ask for evidence

Can we locate the plan without our usual network?

Can someone else contact the provider and authorize work?

Have we tested the service, including sign-in and a normal transaction?

Did we record what failed and who will address it?

Has a system, staff, or contract change invalidated the last result?

Service / evidence date / current level:

Most important unknown:

Next demonstration / owner / locally agreed review date:

A documented plan for one service does not establish readiness for the whole library. Record unknowns explicitly; do not average them away.

Set recovery priorities

Choose the minimum useful service before choosing the technology. Ask who is affected, how harm grows over time, and whether a temporary arrangement is safe and manageable.

Two targets to agree on

Recovery time objective (RTO): the planned maximum time a system resource can be unavailable before its impact is unacceptable. Recovery point objective (RPO): the point in time to which data must be recovered, which describes tolerated data loss. These are planning targets; a test establishes observed performance. [3]

Illustrative example: a library chooses an 8-hour restoration target and a 4-hour data-loss tolerance for a service. A nightly backup alone may not meet that data-loss target. The library and provider must align the targets, backup schedule, and restore capacity.

Complete one service card

Service / accountable owner / alternate:

Minimum useful service and people affected:

RTO / RPO / reason for each target:

Fallback / limits / trigger to stop the fallback:

Dependencies: power, network, sign-in, software, data, people:

Restoration order / provider / acceptance check:

Library-specific decisions

Circulation: can an approved offline procedure work without collecting unnecessary patron information? Public computers: is authentication and session cleanup working? Payroll: does a deadline change its priority? Digital resources: do patrons still have a working route through authentication?

A fallback creates work too. Decide who secures temporary records, reconciles them, and applies the library's retention policy. Do not collect payment-card details in an improvised paper log.

Choose backups you can restore

CISA recommends offline, encrypted backups and regular checks of their availability and integrity. It also recommends exercising response and communication plans and keeping offline copies. [1]

Offline removable media

Potential fit: modest data volumes and a disciplined staff routine. Ask who rotates media, protects off-site copies, can obtain recovery keys, and notices a missed run. Include staff time and replacement media in cost comparisons.

Managed cloud backup

Potential fit: off-site storage with provider support. Verify what is covered, retention, deletion protection, account recovery, export options, restore charges, and how long a full download would take. Confirm whether compromised production credentials could also remove backups.

Local backup appliance or recovery host

Potential fit: faster local recovery or larger data volumes. Check the need for a separate off-site copy, replacement hardware, maintenance, and isolation from affected accounts and networks. Nearby equipment may be lost in the same building event.

Hosted application recovery

Potential fit: the provider manages the application and its recovery. Obtain evidence about your library's data, tenant-level recovery, retention, and export. Do not assume a service subscription or synchronization feature includes the recovery you need.

A useful restore test

Arrange a safe test outside production. Recover representative data and the application dependencies, then have staff complete a realistic transaction. Record elapsed time, restored data date, errors, and missing access. Protect sensitive test data and dispose of it under approved procedures.

The British Library reported viable backup data but insufficient viable infrastructure on which to restore it after its 2023 attack. Legacy software and support constraints complicated recovery. The lesson is to test a working service, not just the existence of files. [4]

Choose a combination that meets your tested needs. No single storage label proves recoverability, and a successful backup job is not a successful restore.

Make vendor dependencies visible

For each critical service, ask the provider to complete these questions with you. Include consortia, municipal IT, identity providers, and network carriers where relevant. One contract rarely describes the whole service.

Contact and authority

Who accepts an urgent incident after hours? What is the escalation route if that person does not respond? Who at the library may approve work? Does the agreement cover incident response, restoration, or only routine support?

Recovery responsibilities

Who restores data, application configuration, authentication, licenses, and integrations? What must the library supply? Which subcontractors or upstream services must recover first? What happens if the ordinary administrator cannot sign in?

Evidence and costs

What recovery targets are contracted, and what recent tests support them? Are they for the provider's platform or our library's service? What are the emergency labor, data retrieval, replacement, and migration costs? Who approves charges before work begins?

Data and exit arrangements

What can we export, in what format, and who can use it? What is excluded? How are incidents communicated? What happens if support ends or the provider becomes unavailable? Ask for written answers where the contract is unclear.

Keep a dependency record

Service / provider / support reference:

Primary and alternate contact / after-hours route:

Prerequisite services / library responsibilities:

Written recovery commitment / evidence / unresolved gap:

Keep a protected offline contact sheet. Record where authorized staff can obtain credentials securely; do not put passwords, recovery codes, or private keys in this playbook.

Communicate useful facts

Tell each audience what has changed, what they should do, and when they will hear more. Maintain one dated service-status record. The wording below is a template to adapt, not a statement about a real incident.

First public update

As of [date, time, time zone], [services] are unavailable. You can still [confirmed available services]. Please [use this temporary arrangement / avoid this action]. We are working with [appropriate description of response partners] to assess the disruption. Our next update will be posted at [location] by [time], even if there is no change.

Staff handoff

Confirmed facts: [observations and service status].

Current instructions: [approved workarounds and actions to avoid].

Questions and unusual activity: report to [role and trusted channel].

Public questions: use [approved update] and refer other questions to [spokesperson].

Next staff update: [time and channel].

Leadership decision request

We need a decision on [service, spending, or staffing choice] by [time]. The confirmed impact is [impact]. Options are [choices and tradeoffs]. Our recommendation is [action and reason].

Unknowns that may change this decision are [unknowns].

Keep uncertainty visible

Say that investigation is continuing when it is. Do not claim that no information was accessed or that a system is safe until the responsible responders can support that statement. Avoid naming a suspected attacker or publishing technical details that could hinder response.

Use a channel that will survive the incident: an independently hosted status page, phone greeting, printed signs, or an agreed partner channel. Provide the same practical information in accessible formats and the languages your patrons need.

Spokesperson / alternate / approval route:

Primary status channel / fallback / next update time:

Practice before it happens

These are fictional tabletop scenarios, not accounts of actual incidents. Suggested format: 30 minutes of discussion, followed by 15 minutes to record gaps. Do not disable live systems to make an exercise feel realistic.

Scenario 1 / Internet outage on a busy afternoon

The building is open, but the catalog, public internet, and cloud-based phone system are unreachable. The carrier has no restoration estimate. A patron needs to submit a time-sensitive application.

Discuss: Who distinguishes a carrier outage from a local failure? Which services continue? How do staff contact support without the phone system? Is an approved alternate connection or partner location available? What will the sign on the door say?

Success check: staff can explain one safe fallback and reach the provider without using the failed connection.

Scenario 2 / A ransom message before opening

A staff workstation displays a ransom message. Shared files cannot be opened. The usual technical contact is away, and someone suggests restarting everything.

Discuss: Who activates the major-incident response? How will qualified responders coordinate containment? Which communication channel is trusted? Who protects evidence, contacts response partners, and approves public wording? What would justify reopening a service?

Success check: the alternate locates the plan, reaches the response contact, and identifies decisions that must wait for technical assessment.

Scenario 3 / Water damage with usable backups

A leak damages local equipment over a weekend. The backup provider confirms a recent copy, but replacement hardware is unavailable and a needed software installer cannot be found.

Discuss: Who determines safe building access? Which services depend on the damaged equipment? Can a supported temporary environment be arranged? Who can approve costs? How will staff verify recovered transactions?

Success check: the team identifies the missing recovery dependency and assigns an owner to resolve it, rather than recording only that backups exist.

End each exercise with one priority fix, an owner, an agreed review date, and a demonstration that will show whether the fix worked.

Spend where it closes a gap

Start with the smallest investment that resolves a demonstrated obstacle to an essential service. The phases below are suggested sequencing, not price quotes, funding promises, or mandatory deadlines.

Use existing resources first

Confirm contacts and alternates. Write one service card. Locate contracts, licenses, and restoration instructions. Agree on emergency authority. Prepare a status message. Run a short tabletop and identify the most consequential unknown. These steps still require paid staff time.

Fund a focused demonstration next

Ask for a bounded quote to restore one priority service in a safe test environment. Include library staff validation. If the test reveals missing off-site protection, unavailable recovery keys, or obsolete software, use that evidence to prioritize the next purchase or support agreement.

Consider larger recurring commitments

Compare managed recovery support, protected off-site backups, replacement reserves, and alternate connectivity against service needs. Include labor, training, restore fees, storage growth, subscriptions, maintenance, and exit costs. A lower subscription fee can leave expensive recovery work outside scope.

A proposed first-month sequence

Week 1: choose one service; confirm owner, authority, and contacts.

Week 2: map dependencies and agree on recovery targets with the provider.

Week 3: exercise the plan and conduct an authorized restore test if ready.

Week 4: review evidence, fund the highest-impact gap, and set the next check.

Make a specific funding request

We need [resource] because [observed gap] prevents [essential service] from meeting [locally approved target]. The estimated total cost is [quote plus staff time and recurring costs]. We will verify the benefit through [service test]. The remaining risk is [unresolved limitation].

First priority / evidence / proposed owner:

Cost to obtain / decision-maker / review date:

Record what recovery proved

Use this sheet after an exercise or restoration. Record enough evidence for another person to understand the result. Keep sensitive investigation records in the approved restricted location.

Incident or exercise / date / lead:

Service / intended RTO and RPO:

Restoration start / usable-service time / elapsed time:

Restored data timestamp / observed data loss:

Representative transaction tested / staff validator:

Dependencies that worked / failed / remain untested:

Before reopening

[] Technical lead confirms the recovery environment is ready for the proposed use, with unresolved risks documented.

[] Service owner verifies the normal workflow, access permissions, and affected integrations; temporary records have a reconciliation plan.

[] Authorized lead records acceptance, any service limits, and the time of the next check. Staff and patrons receive an updated service notice.

Reopening decision / approver / restrictions:

Turn the finding into a repair

Highest-impact gap / action / owner / agreed due date:

Evidence needed to close it / next review date:

Record partial recovery as partial. A test of one sample or one service does not establish that every record, integration, or system has recovered. Retest after a relevant change or a failed check.

Sources and scope

Sources checked October 19, 2026. The historical case describes the state reported in March 2024, not the library's current service status. Numbered references identify the documented claims in this playbook.

[1] CISA and partners / #StopRansomware Guide

October 2023 guide, especially pages 5-6 and the response checklist. Basis for offline encrypted backups, restore checks, offline plans, coordinated isolation, and separate response communications. Links below include the official guide page and a government-hosted PDF.

[Official guide](#)

[Government-hosted guide PDF](#)

[2] NIST / SP 800-61 Revision 3

Incident Response Recommendations and Considerations for Cybersecurity Risk Management, April 2025. Basis for integrating incident response into ongoing risk management.

[Publication and full text](#)

[3] NIST / SP 800-34 Revision 1

Contingency Planning Guide for Federal Information Systems, 2010. Sections 3.2, 3.4, 3.5, and 4 provide context for recovery objectives, dependencies, testing, and reconstitution. Federal guidance is adapted here as a planning resource, not presented as a library mandate.

[Full guide](#)

[4] British Library / Cyber incident review

March 8, 2024, especially printed pages 7-9. First-party account supporting the backup-versus-infrastructure lesson on page 6.

[Published incident review](#)

The maturity levels, incident levels, scenarios, worksheets, budget sequence, and sample communications are proposed library-specific adaptations. They are not endorsed scoring systems or reports of implementation at NEKLS. This resource complements the Disaster-Proofing the Library presentation; it is not a reproduction of a book chapter.

Use this playbook with your library's emergency procedures, technology agreements, and locally approved service priorities. Review contacts and recovery arrangements after relevant staffing, system, or contract changes.