Backup and restoration policy with test plan

Policy and checklist | English · Template to adapt | v3.0 · 2026-10-16

Template version: 3.0. Type: policy and operational procedure. Proposed profile: an organization of approximately 80 people whose operations, hosting or backups may be outsourced. This makes no claim about your environment. Internal owners retain business objectives, gap acceptance and recovery authorization even when a provider performs every technical operation.

After adaptation and adoption, “must” and operational instructions are internal requirements within approved scope. Before adoption they remain proposals. Frequencies, retention, RPO/RTO objectives, windows and criteria require local decisions. This model guarantees neither compliance, complete recovery nor a recovery time. A successful job alone does not establish that a service can be restored.

1. Purpose, scope and adoption decisions

The policy must cover data, configurations, applications and resources needed for priority activities. Identify what requires reconstruction, recovery or reinstallation from a controlled source. Scope must include outsourced services, endpoints holding unique data, directories, keys, catalogs and procedures where needed for selected recovery. Each item must be linked to an activity and an accountable owner.

Distinguish backup, replication, availability and archiving. These mechanisms may support different objectives; their presence does not make them interchangeable. A supplier retaining replicas does not automatically promise required recovery after deletion, compromise or error. Contracts and representative testing must confirm capabilities actually usable, including the organization's access and any provider assistance required.

Parameter	Local decision	Authority	Evidence
Activities and scope	[TO COMPLETE: services, data, dependencies, exclusions]	Management and business	Map and accountable owners
Business objectives	[TO COMPLETE: acceptable loss and interruption]	Business owners	Approved tradeoffs
Copy strategy	[TO COMPLETE: frequency, media, separation, retention]	Internal owner	Verified capacity and protections
Recovery and testing	[TO COMPLETE: scenarios, order, criteria, windows]	Business and operations	Procedure and results
Document control	[TO COMPLETE: version, effect, approver, review]	Management	Accessible approved document

Exclusions require reason, owner, risk and action. Verify information before the effective date: a new service, moved data or missing catalog may change recovery. Keep gaps visible. A list of backup jobs does not adequately describe protected services. Adoption must identify the services for which recovery remains unproven rather than silently count them as covered.

2. Responsibilities and absence arrangements

Function	Responsibility	Reserved decision	Absence or failure
Management or delegate	Decide resources and residual risk	Accept gap against objectives	Named internal deputy
Business owner	Define priority, data and operation to recover	Validate minimum service and outcome	Deputy familiar with activity

Function	Responsibility	Reserved decision	Absence or failure
Internal owner	Maintain strategy, coverage, contracts and evidence	Accept readiness and request correction	Deputy with procedure access
Provider or backup team	Execute, check, restore and provide evidence	Act within mandate only	Escalation and authorized operator
Security or incident lead	Assess compromise and safe recovery	Recommend protection and conditions	Identified alternate
Data owner and competent functions	Define sensitivity, access and preservation	Authorize uses and constraints	Alternate advice or owner

The internal owner must check contracted scope, exclusions, support hours, restoration access, retrieval arrangements, return, costs and capacity dependencies. Obtain acceptance of tasks and evidence expectations. Supplier commitments must not become “demonstrated” business objectives without an end-to-end test. The organization must know who confirms the result when the supplier declares execution complete.

Deputies must find contacts, instructions, authority and approved secret-recovery arrangements without using the absent person's account. General documents must not contain those secrets. Assess dependence on the same email or directory as affected systems; test fallback rather than merely describe it. A recoverable backup with inaccessible authority or instructions is still an incomplete operational capability.

3. Define RPO/RTO from business needs

Business owners must explain acceptable data loss and interruption. Translate these needs into local objectives and define when measurement begins. Here RPO means the recovery-point objective governing data loss; RTO means the recovery-time objective. Values must not be selected solely from a software menu. Record the business reasoning and the activity that a proposed objective supports.

Operators must assess whether frequency, application consistency, volume, capacity, bandwidth, keys and access support objectives. Include preparation and dependencies within the approved measurement scope. If capacity is insufficient, present gaps and options. Management must decide resources, priority or risk; objectives must not silently change to match the latest result. Keep original and revised decisions distinguishable.

Activity	Need to express	Technical verification	Decision if unmet
Order processing	Necessary data, acceptable loss, minimum operation	Consistent copy and representative transaction	Additional capability or accepted degraded service
Identity and administration	Access needed for other recovery	Directory, emergency accounts and authority	Revise order and dependencies
Hosted data	Period, granularity and available access	Actual export/restoration	Contract, other protection or accepted risk
Unique local data	Unsynchronized sources and owner	Inclusion or controlled retrieval	Remove uniqueness or document exclusion

Each service needs a record covering owner, components, dependencies, objectives, copies, retention, sequence, method and test. Business and technical owners approve values jointly. Faster but inconsistent restoration may not meet the need; a recent file without its application or key is not a recovered service. Test evidence must therefore address both data and usable business function.

4. Design copies and separation

The strategy must identify copies for accidental deletion, equipment failure, site loss and compromise. Identify administrative control capable of modifying or deleting each copy. A connected offsite copy is not an offline copy. Check actual permissions and paths, including supplier and production identities. Location alone does not demonstrate separation from the credentials or administrative system under threat.

Examine claimed immutability: mechanism, configured period, who can change it, account deletion, keys and provider conditions. Do not use the label as an absolute guarantee. Modification protection and disconnected copies may be combined according to risk; choices and limits require approval and authorized tests. The organization must know which scenario each protection addresses and which remains uncovered.

Protection	Question to verify	Evidence	Failure treatment
Network separation	Can production access reach the repository?	Configuration and authorized check	Restrict or explicitly accept risk
Distinct identities	Could a compromised account delete copies?	Roles and refusal test	Revise privileges and fallback
Modification protection	Who changes rules and for which period?	Settings, rights and planned test	Correct protection or limit claim
Offline copy	When is it truly disconnected and retrievable?	Inventory, custody and read test	Arrange rotation or another strategy

Copies must receive protection appropriate to data sensitivity. Encryption requires recoverable keys and authorized access. Consider stolen media, corruption, supplier change and loss of identity. Protecting a copy does not remove the need to inspect its contents and know how to restore it. The strategy must distinguish confidentiality protection from usable recovery capability.

5. Protect backup resources and the recovery chain

Administer backup infrastructure with dedicated identities and limited privileges. Separate reading, daily operation, configuration and deletion where capabilities permit. Record sensitive changes and operations. Components must follow patch-management arrangements; protecting data while neglecting backup software leaves a critical dependency untreated. The internal owner must obtain evidence of maintained versions and relevant configuration changes from the provider.

Preserve resources needed to rebuild the facility: procedures, catalog, configuration, authorized installation media, licenses, equipment or capacity, import mechanisms and key recovery. Protect fallback resources while keeping them usable by authorized people. An encrypted copy without a recoverable key does not demonstrate restoration capability. The plan must name who can authorize and perform recovery of protected key material.

Dependency stage	Necessary input	Check	Owner
Emergency access	Identity, delegation and authenticator	Authorized access without affected system	Internal owner
Infrastructure	Controlled network, time, storage and administration	Available resources, isolated if needed	Operator
Tool and catalog	Installation resources and copy references	Copy located and readable	Backup team
Keys and data	Authority, key and consistent point	Decryption and integrity checked	Custodian and operator

Dependency stage	Necessary input	Check	Owner
Application	Versions, settings and dependencies	Technical function, then business operation	Technical and business owners

Sequence depends on the service; this chain is an adaptable model, not a universal order. Identify circular dependencies, such as instructions or secrets accessible only through the application being restored. Test alternative access and assign correction. Unresolved dependencies must remain explicit recovery reservations. A diagram does not replace an executable procedure and a tested route through its prerequisites.

6. Run backups and handle failures

Check jobs, actual included data, freshness and unusual volume, duration or configuration. Green status may exclude a volume or application. Compare actual scope with service records and recent changes. Link supplier messages to affected services rather than merely archive them. Monitoring must identify who receives a failure and what decision they are expected to make.

Observation	Action	Evidence to retain	Escalation
Failed job	Identify state, cause and remaining usable copy	Error, service, last useful point	Internal and business owners according to exposure
Successful job, doubtful content	Compare inclusion with expected data	Scope difference and check	No complete-protection claim
Stale copy	Compare with approved objective	Last consistent point and potential loss	Protection decision or accepted risk
Unexpected change	Check authorization and effect	Configuration, actor and history	Security if compromise plausible

Every failure requires owner, action and reassessment. Verify the next successful job before closure. When the service exceeds its approved objective, inform business owners of potential loss and obtain a decision with the relevant authority. Repeated retries without diagnosis must not conceal sustained absence of a usable copy. Keep previous errors so the history explains what happened.

Providers must confirm both execution and checks. If unavailable, use planned escalation and fallback. Alternative methods must not expose data through unauthorized export. Waiting risk and missing capability require an internal decision-maker, not silent acceptance. The owner must record what remains protected, what is uncertain and the next attempt or protective measure.

7. Select and authorize restoration

Requests must specify service, data, reason, desired point, destination and authority. Verify need, requester's rights and risk of overwriting newer data. Restoration to another user or system requires specific permission. Recovery must not become a route around ordinary access restrictions. Preserve the authorization so operators do not rely solely on an urgent request from an unverified account.

Identify copy, age, dependencies and application consistency. Approve environment, window, impact, success criteria and stop conditions. Preserve source state and useful current data as appropriate. Distinguish a restoration test, recovery of an item and complete service recovery; they need different evidence. The record must name the person who validates the selected level of recovery.

Branch	Authority and preparation	Outcome check	Reservation
Deleted item	Data owner; separate destination where appropriate	Content and access accepted	Not proof of complete reconstruction

Branch	Authority and preparation	Outcome check	Reservation
Technical outage	Business and operations; dependencies and capacity	Application and representative operation	Effects on recent data
Compromise	Incident lead; controlled environment	Security checks and conditional recovery	Copy may be contaminated
Supplier request	Mandate, scope and protected transfer	Readable receipt complete for requested scope	Unconfirmed capability or retrieval time

8. Recover after compromise

The incident lead must coordinate preservation, backup protection and reconstruction. Copies may contain malicious implants or hostile configuration; age or readability does not establish cleanliness. Selection must use available evidence about the compromised period and record unknowns. An antivirus check alone is not a guarantee of safety. Explain which security checks support the chosen recovery point.

Use controlled reconstruction appropriate to capability: verified installation sources, reviewed configuration, checked data before import and administration independent of suspect access. The lead decides necessary restrictions and monitoring. Prepare backup-infrastructure isolation with operators and understand its effects instead of improvising during crisis. Protecting copies and preserving recovery capacity must be coordinated with business continuity and incident response.

Recovery gate	Required evidence	Authority	If insufficient
Prepare	Identified administration, environment and copy	Lead and operator	Defer or restrict scope
Restore	Justified method, keys and point	Authorized operator	Keep error and reassess
Verify	Integrity, access, data and business function	Technical and business owners	Repair, change point or degrade service
Reconnect	Suspect access addressed, risks and monitoring	Recovery authority	No expansion without decision
Finish	Criteria met; remaining work assigned	Management or delegate	Explicit residual-risk acceptance

Recovery does not replace investigation or treatment of hostile access. Business owners must understand what returned and what remains missing. Define stop conditions if suspicious signs appear. A technically completed rebuild must not be called normal service before agreed validation. Keep security and business reservations visible in the authorization to expand or reconnect.

9. Test capability, not merely a copy

The program must cover representative risks: file, application, identity dependency, loss of ordinary tools and cyber recovery where relevant. Select tests with business and operations, decide local scope and frequency and explain exclusions. A file test must not be presented as full reconstruction. Prioritize tests that exercise critical dependencies and previously unproven assumptions.

Authorization must specify test data, environment, real-message risks, temporary access, stop conditions and end-of-test deletion. Avoid reactivating suspect accounts, sending to real recipients or overwriting production. Record stage start and end within the measured scope. Include waiting and preparation rather than measuring only byte transfer. State any excluded time so comparisons remain interpretable.

☐ Confirm authority, scenario, scope and fallback people.

☐ Find procedure, catalog, copy, keys and capacity without blocking dependency.

☐ Check test separation and data protection.

☐ Execute stages; retain errors, durations and adjustments.

☐ Verify data, access and business operation.

☐ Compare observed loss and time with approved objectives.

☐ Assign gaps and schedule another check.

☐ Remove temporary access, delete test data and confirm closure.

Another person must be able to understand what the report actually demonstrates. Identify service, point, environment, operator, reviewer, criteria, gaps and decision. Business owners must accept or reject the result. An inconclusive test can be valuable when it exposes a specific dependency and produces verified correction. A completed report without evidence must not substitute for the exercised capability.

10. Complete fictional recovery scenario

Fictional Atelier Rivage has approximately 80 staff and must recover order processing after suspected compromise. Its business owner has set local objectives without universal values. The provider has copies, but the initial procedure depends on unavailable email. The deputy uses a controlled fallback copy. This scenario is not customer experience or evidence that a real deployment meets any target.

Fictional stage	Observed state	Decision and owner	Evidence
Preparation	Catalog available; email unavailable	Lead uses fallback channel and procedure	D-01, authorized access tested
Copy selection	Recent point falls in suspect period	Security reserves its use; another point examined	E-01, reasons and unknowns
Reconstruction	Tool and keys recovered in separate environment	Provider executes mandate	E-02, reading and decryption
Business test	Test order works; attachment missing	Business rejects normal service and accepts bounded degradation	D-02, assigned gap
Validation	Missing data recovered; check repeated	Authority expands with monitoring	D-03, check and remaining risk

Acceptance requires the deputy to explain copy selection, locate decryption authority and show why the first result was not complete recovery. Distinguish a backed-up workload, recovered data and validated service. Identify correction and next check instead of declaring success because the tool finished. The exercise must preserve the rejected initial acceptance and the reason for the later decision.

11. Adaptable registers and exceptions

Blank service record	Local value	Owner	Verification
Need and dependencies	[TO COMPLETE: activity, minimum, order, suppliers]	[TO COMPLETE]	Business and technical assessment
Objectives	[TO COMPLETE: RPO/RTO, measurement start, reason]	[TO COMPLETE]	Internal approval
Copies and access	[TO COMPLETE: frequency, separation, keys, retention]	[TO COMPLETE]	Read and refusal tests

Blank service record	Local value	Owner	Verification
Restoration	[TO COMPLETE: method, destination, checks, stop]	[TO COMPLETE]	Technical and business result
Test and gaps	[TO COMPLETE: scenario, observations, decision, follow-up]	[TO COMPLETE]	Acceptance and correction

Exception	Completed fictional example	Local adaptation	Decision-maker
Unmet requirement	No disconnected copy for a secondary service	[TO COMPLETE]	Internal authority
Compensation	Protected copy and restricted access tested; limitation retained	[TO COMPLETE]	Security and business consulted
Risk and exit	Excessive privilege may still destroy copies; change planned	[TO COMPLETE]	Named acceptance
Expiry and check	Actual local date required before signature; reassess after change	[TO COMPLETE]	Action owner

Exceptions must state cause, scope, risk, verified compensation, owner, expiry and review. A provider cannot alone accept gaps against business objectives. At expiry obtain correction or a new decision; silent renewal is prohibited. Assumed protection must not be called verified compensation. The register must expose which failure remains possible and how the decision-maker understood that limitation.

12. Oversight, enforcement and revision

At [TO COMPLETE: body and cadence], report uncovered services, old copies, failures, insufficient capacity, overdue tests and exceptions. Indicators must state population, period and limits. Keep “job executed,” “data recovered” and “service restored” distinct. Unknown state must not count as compliant. Management must receive the decision required and the consequence of leaving the gap unresolved.

Examine unauthorized restoration, excessive access or ignored failure with competent functions. Protect data, assign correction and verify follow-up. This model creates no automatic sanction. Responses follow internal rules, contracts and applicable obligations while preserving useful evidence. Supplier actions and internal decisions must remain distinguishable when the cause or treatment of a process gap is reviewed.

Review after incidents, inconclusive tests or changes to dependencies, identities, keys, suppliers or objectives. Retain author, reason, approver and superseded version in [TO COMPLETE: repository, access, retention]. Distribute approved instructions to operators and deputies. Verify return and recovery during supplier exit before losing necessary technical resources. A replacement contract must not erase the history of unproven recovery capability.

Primary sources and limitations

The ANSSI backup guide, version 1.1 of 27 November 2025, notably §2 and R1–R32, addresses objectives, separation, identities, testing, recovery order and compromised copies. NIST SP 800-34 revision 1, published in 2010, provides planning and testing context requiring adaptation to current technology.

Proposed roles, tables, scenarios and criteria are organizational choices, not guarantees or certification. Verify provider mechanisms, application consistency, safety and obligations in your environment. Objectives may require capability beyond backup alone. Local approval and a useful document do not replace testing of the actual recovery chain.