

Request for Proposal: Immutable Backup Storage and Cyber

Recovery Vault

Template from RFPhub.com. Replace everything in square brackets, adjust the Must-have/Nice-to-have priorities, and delete this note and the instructions section before you issue the RFP.

Instructions for the buyer (delete before issuing)

An immutable backup and cyber recovery vault evaluation sits between the backup, storage and security teams, and the decisions that matter most (which data goes in the vault, how isolated it is, and how fast you need it back) should be settled before vendors get involved. The example schedule below runs about 13 weeks from kickoff to contract award; stretch it if your proof of concept includes a full clean-room recovery of several applications.

1. **Define data tiers and recovery objectives (weeks 1-2).** List your critical applications and data sets, and decide which need an immutable copy and which also need a vaulted copy. Set retention for each tier, note any regulatory retention periods, and agree on recovery time and recovery point objectives for recovery from the vault, not just from normal backups. Record the numbers vendors will price against: protected data volume, daily change rate, retention and expected growth.
2. **Assemble the buying team.** Include backup and storage administrators, security operations and incident response, the identity and network teams (they will design the vault's isolation), owners of the critical applications, risk and compliance, procurement and legal. Add whoever handles cyber insurance if your policy asks about backup controls. Decide early who will hold the vault's credentials and who will approve destructive actions, because those people can't be the same.
3. **Choose the architecture, and decide whether you need an RFI (weeks 2-4).** Decide whether you need an immutable target for your existing backups, an isolated vault as well, or both, and whether the vault will be on premises, in a cloud account you control, or a vendor-hosted service. If

you're unsure, or your long list mixes storage appliances, software-defined storage and hosted vault services, issue a short RFI first asking how each vendor's locks work, what isolation it provides and how it prices, then build a shortlist of three or four.

4. **Tailor and issue the RFP (weeks 4-7).** Delete requirements that don't apply, adjust priorities, and add your backup software versions, data volumes and retention periods to Section 1. If you only need an immutable target, mark the vault and clean-room requirements Nice-to-have or delete them. Give vendors three weeks to respond, with a written question-and-answer window in the first week.
5. **Score the responses (weeks 7-8).** Have each evaluator score independently against the rubric before comparing notes, and set aside any vendor that misses a Must-have. Check every 'immutable' claim: is the lock enforced by the storage itself in compliance mode, or is it a setting in the backup software that an administrator could change? Check which features are generally available today and which are on the roadmap.
6. **Run a proof of concept with two vendors (weeks 8-12).** Try to delete locked backups and shorten retention with your most privileged account, then again from a backup server you treat as compromised. Simulate an attack: encrypt a test data set, let it be backed up, and see whether detection alerts fire, whether the last clean restore point can be found, and how long recovery into the clean room takes. Measure restore throughput with your own data, and call a reference customer that has recovered from the vault.
7. **Negotiate and award (weeks 12-13).** Use the pricing table to compare like for like. Settle recovery-time charges (data retrieval, egress, clean-room compute), capacity growth pricing, renewal caps, hardware refresh terms and what happens to locked data at the end of the contract before you sign.

Immutable storage, air gaps and cyber recovery vaults: what's the difference?

Immutable backup storage stops backup data from being changed or deleted before its retention period ends. WORM (write once, read many) is the general term. On object storage, the standard mechanism is object lock in the S3-compatible API: in compliance mode no user, including administrators, can shorten retention or delete locked data before it expires, while in governance mode users granted a specific permission can override the lock. A hardened appliance goes further by locking down the operating system itself, for example by removing root

and shell access, so a compromised administrator account can't get underneath the lock.

Immutability doesn't isolate the data. An attacker who controls your backup console, identity system or network can still stop new backups, shorten retention on future copies, or reach the encryption keys you need to restore. An air gap adds isolation. A physical air gap keeps a copy on offline media. A logical air gap keeps a copy on a network and management plane that production can't reach, with replication opened only on a schedule and from the vault side.

A cyber recovery vault combines both: an immutable, isolated copy of your most critical data with its own credentials, plus the tools to use it after an attack, such as malware scanning, a way to find the last clean restore point, and a clean room where systems are rebuilt before they reconnect to production. This template covers immutable storage and the vault. If you only need an immutable target for your existing backups, mark the vault and clean-room requirements Nice-to-have or delete them.

Questions to settle before you issue the RFP:

- Which data sets need a vaulted copy, not just an immutable one?
- How long must locked copies be kept, and does any regulation or contract set the period?
- Will the vault be on premises, in a cloud account you control, or a vendor-hosted service?
- Who will hold the vault's credentials, and who will approve destructive actions?
- Where will the clean room run, and who will build and maintain it?

Contents

1. Introduction and Background
2. Project Objectives
3. Scope of Work
4. Requirements
5. Vendor Questions
6. Evaluation Criteria and Scoring
7. Pricing Response

8. Submission Guidelines

9. Timeline

1. Introduction and Background

[Company Name] is seeking proposals for immutable backup storage and a cyber recovery vault that keep our backup copies from being altered or deleted before their retention expires, hold an isolated copy of our critical data, and let us scan, validate and recover clean data after a cyber attack. This RFP describes our requirements, the questions we need answered, and how proposals will be evaluated.

Organization background

- [Describe your organization: industry, size, locations]
- [Regulatory or contractual requirements that apply]
- [Current backup software, versions and backup repositories in use]
- [Volume of protected data, daily change rate and expected growth]
- [Retention requirements by data type, including any regulatory retention periods]
- [Critical applications and data sets that need a vaulted copy, with their recovery time and recovery point objectives]
- [Data centers, cloud accounts and regions where storage, the vault and a clean room could run]
- [Identity provider, key management system, SIEM and incident response arrangements]

2. Project Objectives

- Keep backup copies that cannot be modified, encrypted or deleted before retention expiry, including by administrators
- Hold an isolated copy of critical data that production credentials and networks cannot reach
- Detect malware, mass encryption and suspicious administrative activity affecting backup data
- Recover critical applications from a verified clean copy within our recovery time objectives

- Produce evidence of immutability, retention and recovery testing for auditors, regulators and insurers

3. Scope of Work

The selected vendor will be responsible for:

- Delivery of immutable backup storage with [initial capacity] usable, expandable to [target capacity]
- Design and deployment of an isolated cyber recovery vault for [critical data sets], with scheduled replication from production
- Design of the clean-room recovery environment and recovery runbooks for [critical applications]
- Integration with our backup software, key management, identity, SIEM and ticketing systems
- A proof of concept, followed by phased migration of in-scope backup jobs, in phases agreed with [Company Name]
- Training for backup, storage and security staff, and ongoing support for the contract term

4. Requirements

For each requirement, enter a response code and a short explanation. Y = available today in the proposed edition; P = partially met or needs configuration/services (explain); R = on the roadmap (give a date); N = not supported. Must-have requirements are pass/fail; Nice-to-have requirements add points.

4.1 Functional

ID	Requirement	Priority	Response	Vendor comments
F1	Immutability enforced by the storage platform itself, not only by the backup software: locked backup data can't be modified, overwritten, encrypted or deleted until its retention expires, even by someone holding valid backup-server credentials.	Must		
F2	Compliance-mode retention locks (object lock compliance mode or an equivalent WORM setting): once set, no user, including our administrators, the account or tenant owner and the vendor's support staff, can shorten the retention period, remove the lock or delete the data before it expires.	Must		

ID	Requirement	Priority	Response	Vendor comments
	Retention can only be extended.			
F3	Governance-mode locks for lower-tier data, where only named roles with a specific permission can shorten or remove retention, and every override is logged and alerted to the security team.	Nice		
F4	Retention set per object or per backup by our backup software through the API, including extending retention on existing data, plus a default retention per bucket, volume or policy for data written without one.	Must		
F5	Legal hold on selected backups or data sets that prevents deletion regardless of retention expiry until an authorized user releases it, with every hold and release recorded against the user who made it.	Must		
F6	Protection of retention expiry from changes to the system clock or time source (for example, a tampered NTP server). Describe how the platform keeps time and limits clock changes.	Must		
F7	Multi-person authorization for destructive and security-weakening actions, such as deleting data, shortening retention, removing a legal hold, deleting buckets, volumes or policies, changing replication or time settings, resetting administrator credentials and disabling MFA. A second person with separate credentials must approve each one.	Must		
F8	Malware scanning of restore points before they are restored, with signatures kept current in isolated deployments and support for indicators of compromise from our security team (such as file hashes and YARA rules). Results are recorded against each restore point. State whether scanning is part of the proposed solution or relies on our backup software.	Must		
F9	Detection of signs of ransomware in protected data, such as entropy changes, unusual change rates, mass deletions or file-type changes, with alerts to our security team. State whether detection is part of the proposed solution or relies on our backup software.	Must		
F10	Identification of the most recent restore point with no detections for each protected system, to speed up choosing a clean	Nice		

ID	Requirement	Priority	Response	Vendor comments
	recovery point during an incident.			
F11	An isolated recovery environment (clean room) where restore points can be mounted, scanned and tested without connecting to production networks or identity systems.	Must		
F12	Automated clean-room recovery: on-demand provisioning of compute and network on premises or in a cloud account we control, and recovery plans that bring up core infrastructure (directory services, DNS, virtualization management) before applications, with scan steps built in.	Nice		
F13	Read-only access to restore points for our incident responders and forensic tools, without altering the vaulted copy.	Must		
F14	Scheduled recovery tests from the vault with pass/fail results and elapsed times, and reports we can give to auditors, regulators and insurers as evidence.	Must		

4.2 Technical and architecture

ID	Requirement	Priority	Response	Vendor comments
T1	A stated deployment model for each component: on-premises appliance, software-defined storage on our hardware, storage in our cloud account, or a vendor-hosted vault service. Describe where each copy lives and who operates it.	Must		
T2	For appliance and software-defined deployments, a hardened operating environment: no root or shell access for customer administrators, no services beyond those needed, and signed software and firmware updates. State any exceptions.	Must		
T3	A vault copy isolated from production. On-premises vaults: replication initiated from the vault side or through a controlled gateway, with the link closed outside scheduled windows. Cloud or vendor-hosted vaults: a separate account or tenancy with its own control plane. Provide a diagram of every network path into the vault, including management, replication, support and updates.	Must		
T4	A vault management plane separate from production: its own administrator accounts and identity store, MFA for every login, and	Must		

ID	Requirement	Priority	Response	Vendor comments
	management interfaces that can't be reached from the production network or authenticated through our production directory.			
T5	Sustained ingest throughput of at least [value] TB per hour across our backup window, stated for our data mix with deduplication and encryption enabled.	Must		
T6	Restore throughput of at least [value] TB per hour for a mass recovery from the vault, including parallel restores of several applications. State the figures you will demonstrate in the proof of concept.	Must		
T7	Replication of [value] TB per day of changed data to the vault within the scheduled window, with bandwidth throttling and scheduling.	Must		
T8	Capacity reporting and forecasting that account for locked retention, with alerts well before capacity runs out (locked data can't be deleted to free space), and non-disruptive expansion to [target capacity].	Must		
T9	Deduplication and compression, with reporting on data reduction over time. State whether reduction applies to the vault copy and how it interacts with encryption.	Nice		

4.3 Integration

ID	Requirement	Priority	Response	Vendor comments
I1	Validated integration with [current backup software and versions], with a compatibility matrix showing which immutability features are supported for each version.	Must		
I2	A documented S3-compatible object storage API with object lock support (compliance and governance retention modes, retention periods, legal hold and default bucket retention). List any object lock or versioning API calls that are not supported.	Must		
I3	File protocol access (NFS or SMB) where required, with a description of how retention locks are applied and enforced over these protocols.	Nice		
I4	No loss of backup-software features such as synthetic full backups, incremental-forever	Must		