

Request for Proposal: Microsoft 365 Backup and Recovery

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)

What you're really buying is the ability to restore, so agree on what you need to recover, how quickly and from how far back before vendors get involved. The example schedule below runs about 10 weeks from kickoff to contract award; stretch it if you have several tenants or a Multi-Geo tenant, or if your legal hold requirements are still being settled.

1. **Inventory the tenant and set recovery targets (weeks 1-2).** Count what vendors will size and price against: licensed users, shared and resource mailboxes, archive mailboxes, OneDrive accounts, SharePoint sites, teams, and data volume and growth by workload. Set a recovery point objective and recovery time objective for each workload, a retention period for backups, and any legal hold obligations. List the Microsoft 365 retention policies and holds you already use, so the backup design complements them.
2. **Assemble the buying team.** Include the Exchange, SharePoint and Teams administrators, the identity team that owns Entra ID, security operations, whoever runs backup today, and legal, records management, privacy and procurement. Bring security in early: a backup product needs tenant-wide permissions to read and restore your data, and it holds a full copy of it.
3. **Decide whether you need an RFI (weeks 2-3).** If you haven't decided between Microsoft's native options, a vendor-hosted backup service and software you run yourself, or your long list has more than five vendors, send a short RFI first. Ask which workloads each product covers, where backup data is stored, how pricing is counted and which regions are supported. Use the answers to build a shortlist of three or four.
4. **Tailor and issue the RFP (weeks 3-6).** Delete requirements that don't apply, adjust priorities, and add your tenant numbers to Section 1. Make

Entra ID backup, Multi-Geo support and cross-tenant restore Must-haves if you depend on them. Give vendors three weeks to respond, with a written question-and-answer window in the first week.

5. **Score the responses (weeks 6-7).** Have each evaluator score independently against the rubric before comparing notes, and set aside any vendor that misses a Must-have. For each workload, check exactly which item types are covered, and whether every 'yes' is generally available today or still on the roadmap.
6. **Run a proof of concept with two vendors (weeks 7-9).** Use a test tenant or a pilot group, after security has reviewed the permissions each product requests. Time the first backup of a sample, then test the restores you'd need in a real incident: a single email, a full mailbox, a SharePoint site to a new location, a Teams channel, a simulated mass deletion and, if relevant, a restore into another tenant. Check that permissions, metadata and versions come back intact and that every action appears in the audit log.
7. **Negotiate and award (weeks 9-10).** Use the pricing table to compare like for like. Settle how shared mailboxes and departed users are counted, storage limits, renewal caps and exit terms, including how you'd get your backup data out, before you sign.

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 a backup and recovery solution for our Microsoft 365 data in Exchange Online, OneDrive, SharePoint Online and Microsoft Teams, with independent and immutable backup copies, granular and point-in-

time restore, and retention and legal hold controls. 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]
- [Microsoft 365 licensing and number of licensed users; number of shared, resource and archive mailboxes]
- [Data volume and annual growth by workload: Exchange Online, OneDrive, SharePoint Online, Teams]
- [Current backup, retention, legal hold and eDiscovery tools and policies]
- [Number of tenants, Multi-Geo locations, hybrid identity setup, and any planned tenant migrations or mergers]

2. Project Objectives

- Keep independent, immutable backup copies of all in-scope Microsoft 365 workloads, meeting a recovery point objective of [number] hours
- Restore individual items, mailboxes, sites and teams to any retained point in time within [recovery time objective]
- Retain backup data and apply legal holds for [number] years, independent of Microsoft 365 licenses
- Recover quickly from ransomware, mass deletion or a compromised administrator account
- Produce audit-ready evidence of backup success, restore testing and retention

3. Scope of Work

The selected vendor will be responsible for:

- Backup of [list workloads] for [number] users, [number] sites and [number] teams in [regions]
- The first full backup and ongoing incremental backups, scheduled to work within Microsoft 365 API throttling
- Configuration of backup, retention and legal hold policies agreed with [Company Name]

- Integration with our identity provider, SIEM, ticketing system and eDiscovery tools
- Restore testing before go-live, and training for administrators, help-desk and legal staff
- Ongoing support and service management 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	Backup of Exchange Online user, shared and resource mailboxes, including mail, calendar, contacts and tasks. State any folders, item types or mailbox types that are excluded.	Must		
F2	Backup and restore of Exchange Online archive mailboxes, including auto-expanding archives. State how archives are captured and restored.	Must		
F3	Backup of all OneDrive accounts, including files, folder structure, version history, metadata and sharing permissions.	Must		
F4	Backup of SharePoint Online sites, including document libraries, lists, pages, version history, metadata and permissions. State what is not captured, such as site customizations or managed metadata held outside the site.	Must		
F5	Backup of Microsoft Teams: team and channel settings, messages in standard, private and shared channels, 1:1 and group chats, and shared files. For each, state whether it can be restored back into Teams, to another location, or only exported.	Must		
F6	Backup and restore of Microsoft Entra ID objects and configuration, such as users, groups, app registrations, service principals and Conditional Access policies. State which objects and attributes are covered. Make this Must-have if you need protection for identity configuration.	Nice		

ID	Requirement	Priority	Response	Vendor comments
F7	Coverage of other Microsoft 365 data we use, such as Microsoft 365 Group mailboxes, Planner, OneNote notebooks and public folders. State which are protected.	Nice		
F8	Automatic discovery and protection of new mailboxes, OneDrive accounts, sites, groups and teams, using rules (for example, by group membership or site type), with alerts for anything left unprotected.	Must		
F9	Configurable backup frequency for each workload, with change-based incremental backups after the first full copy, and at least [number] backups per day. State the shortest supported interval for each workload.	Must		
F10	Point-in-time restore: browse any protected mailbox, OneDrive account, site or team as it existed at any retained backup, and restore from that point.	Must		
F11	Granular restore of a single email, calendar item, contact, file, file version, list item or folder, with preview before restore.	Must		
F12	Bulk restore of entire mailboxes, OneDrive accounts, sites or teams, one at a time or many at once, with progress tracking and a completion report.	Must		
F13	Restore in place (with a choice to overwrite, skip or keep both copies), to an alternate location in the same tenant, or to a different user, mailbox or site, with permissions, metadata and version history preserved.	Must		
F14	Restore from one Microsoft 365 tenant into another, with mapping of users, groups and sites and handling of naming conflicts. Make this Must-have if you expect a merger, divestiture or tenant consolidation.	Nice		
F15	Search across backup data by user, location, date range, sender, recipient, subject, file name, file type and keyword, limited by the searcher's role, with export of results as PST for mail and in original formats for files.	Must		
F16	Self-service restore for end users of their own mail and files, with optional administrator approval.	Nice		
F17	Alerts on unusual activity seen in backups, such as mass deletion or likely ransomware	Nice		

ID	Requirement	Priority	Response	Vendor comments
	encryption, with help identifying the last clean restore point.			

4.2 Technical and architecture

ID	Requirement	Priority	Response	Vendor comments
T1	Backup copies held outside our Microsoft 365 tenant, in a separate storage location and security domain, so that a compromised Microsoft 365 administrator account cannot delete or alter them. State where each copy is stored, and whether it can be kept in a cloud storage account we own.	Must		
T2	Immutable backup storage: retention locks that no single administrator, ours or the vendor's, can shorten or remove before the retention period ends.	Must		
T3	Protection against destructive actions: deleting backups, shortening retention, disabling protection or removing a tenant requires approval from a second administrator, or a delay with alerts to named contacts.	Must		
T4	Choice of the region where backup data, search indexes and metadata are stored, to meet our data-residency requirements.	Must		
T5	Support for Microsoft 365 Multi-Geo: back up and restore users and sites in every geography of our tenant, and keep each backup in the region we specify. Make this Must-have if your tenant uses Multi-Geo.	Nice		
T6	Handling of Microsoft 365 API throttling without missed backups, for example by honoring retry instructions and using change tracking. Describe how backup jobs share API capacity with other applications in our tenant.	Must		
T7	Documented time for the first full backup and for incremental backups for a tenant of our size ([users], [TB] by workload), and reporting of the recovery point actually achieved per workload, user and site, with alerts on missed backups.	Must		
T8	Use of supported Microsoft APIs for every workload. Confirm that Exchange Online backup and restore, including archive mailboxes, does not depend on Exchange Web Services (EWS), which Microsoft is phasing out in Exchange Online starting in	Must		

ID	Requirement	Priority	Response	Vendor comments
	October 2026.			
T9	Management of several Microsoft 365 tenants from one console, with data kept separate per tenant and administrator roles scoped by tenant.	Nice		

4.3 Integration

ID	Requirement	Priority	Response	Vendor comments
I1	Single sign-on to the backup console through Microsoft Entra ID using SAML 2.0 or OIDC, so our MFA and Conditional Access policies apply to backup administrators.	Must		
I2	Streaming of backup, restore, alert and administrator audit events to our SIEM in a documented format.	Must		
I3	A documented REST API, plus PowerShell or command-line tooling, for automating backup policies, restores and reports.	Must		
I4	Integration with our ticketing (ITSM) and security automation (SOAR) tools, so failed backups, alerts and restore requests create tickets or start response workflows.	Nice		

4.4 Security and compliance

ID	Requirement	Priority	Response	Vendor comments
S1	A current SOC 2 Type II report and ISO/IEC 27001 certification covering the proposed service, available under NDA.	Must		
S2	Certifications or contract terms required in our sector or region, such as FedRAMP authorization for US public-sector use or a HIPAA business associate agreement for US healthcare. Make this Must-have if it applies to you.	Nice		
S3	Encryption in transit and at rest, separation of our data from other customers' data, and a documented key-management approach. State whether customer-managed keys are supported.	Must		
S4	Role-based access control with predefined and custom roles (for example, backup operator, restore operator, legal reviewer and auditor), scoped by workload, user group or geography.	Must		
S5	A complete, tamper-evident audit log of	Must		