Microsoft 365 Backup Policy

[Company Name]
[Date Implemented]

1. Purpose

This policy defines how [Company Name] protects and recovers Microsoft 365 data to ensure business continuity, ransomware resilience, and compliance.

Microsoft 365 provides service availability but does not guarantee long-term backup or point-in-time recovery for all data scenarios. For this reason, the organization maintains an independent backup system for Microsoft 365 data in order to:

- Prevent data loss
- Recover from ransomware
- Protect against accidental deletion
- Maintain regulatory compliance
- Ensure business continuity

---

2. Scope

This policy applies to all Microsoft 365 data owned or managed by [Company Name], including:

- Microsoft 365 users
- Exchange Online mailboxes
- OneDrive accounts
- SharePoint sites
- Microsoft Teams data
- Administrators and IT partners

All employees, administrators, and IT partners must follow this policy.

---

3. Backup Requirements

Backup Coverage

The selected Microsoft 365 backup software must back up:

- Email messages, attachments, contacts, and calendars
- OneDrive user files
- SharePoint document libraries

Backup Frequency

- Backups must run automatically at least once per day.
- Mission-critical data should support multiple backups per day where possible.
- Backups must not require manual user intervention.

Retention Requirements

Backups must exceed Microsoft's native retention limits. [Company Name] will maintain:

- Minimum retention: 1 year
- Recommended retention: 7+ years depending on regulatory requirements

Retention settings must support granular point-in-time recovery.

Recovery Objectives

The backup solution must support:

- individual email or file recovery
- folder or document library restore
- full mailbox restore
- SharePoint site recovery
- point-in-time restore
- rapid search and recovery functionality

Target Objectives:

- Recovery Time Objective (RTO): _____ (Recommended: Under 4 hours)

- Recovery Point Objective (RPO): _____ (Recommended: Under 24 hours)

Actual recovery times must be validated through regular restore testing.

---

4. Security & Compliance

The Microsoft 365 backup system must provide:

- immutable backup storage
- encryption in transit and at rest
- role-based access control
- MFA for administrative access
- audit logging of backup and restore activity
- storage isolated from the production tenant where possible

These controls ensure backups remain recoverable during ransomware or account compromise.

---

5. Monitoring and Ownership

The IT administrator or MSP is responsible for:

- monitoring backup job status
- reviewing backup health alerts
- resolving failed backup jobs
- maintaining documentation of backup configuration

Backup failure alerts must be automatically generated and reviewed daily.

Employees

- Report data loss incidents
- Follow data security policies

---

6. Testing & Validation

To verify recovery readiness:

- Quarterly restore tests must be performed
- Annual disaster recovery simulation must be conducted
- Backup status must be reviewed monthly

Test results should be documented for audit and compliance purposes.

Example Restore Test Record

Test Date	Data Type	Restore Type	Result	Recovery Time
Jan 12	Exchange mailbox	Full mailbox restore	Successful	38 minutes
Feb 3	SharePoint site	Folder restore	Successful	12 minutes

---

7. Ransomware & Incident Response

If a ransomware incident affects Microsoft 365 data:

1. Isolate affected accounts or systems
2. Disable compromised credentials
3. Verify backup integrity
4. Identify the last known clean restore point
5. Restore affected data
6. Document incident and remediation

---

8. Policy Review Schedule

This policy must be reviewed:

- Annually
- After any major Microsoft 365 configuration change
- After any security incident

- When changing backup vendors

Implementation Checklist for Small Business

☐ Select Microsoft 365 backup software for small business
☐ Configure automated daily backups
☐ Enable immutable storage
☐ Define retention period
☐ Test restore process
☐ Document incident response procedure
☐ Review your Microsoft 365 backup policy as per the schedule above

© Copyright CrashPlan 2026 I crashplan.com