

Stork365

Microsoft 365 Backup & Restore: Exchange, OneDrive, SharePoint, Teams & Entra ID

“Your Microsoft 365 data, your storage.” Recover a mailbox, a file, or an identity, without vendor lock-in.

Service	Stork365: Microsoft 365 Backup & Restore
Focus	Workload-aware backup of Exchange, OneDrive, SharePoint, Teams and Entra ID into storage you control
Version	1.0
Date	June 2026
Coverage	GDPR · KVKK · DORA · ISO 27001 · SOC 2
Provider	BackupSec

1. What is Stork365?

Stork365 is a cloud backup service for Microsoft 365. It connects to your tenant through Microsoft Graph and backs up Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, and Entra ID, each with its own workload-aware restore semantics, not a flat file dump. Encrypted copies are written to storage you choose and control (BYOS), and you recover exactly what you need (a message, a file, a site, or an identity) from a single console. Stork365 is the Microsoft 365 protection layer of the BackupSec family, alongside ZeroMON monitoring, ZeroTAM advisory, ZeroPEN penetration testing, and ZeroVault S3-compatible storage for immutable Veeam backups.

Why Stork365? Microsoft’s native retention is not a backup. Deleted items age out, ransomware encrypts synced files, and offboarded identities disappear. Stork365 keeps an independent, encrypted copy in storage you control, recoverable item by item, long after Microsoft’s own recycle bins expire.

The BackupSec family

Stork365 works alongside the rest of the BackupSec family:

Service	Role
ZeroMON	Backup monitoring & observability: real-time visibility across your Veeam estate
ZeroTAM	Expert advisory, account management & crisis support
ZeroPEN	Backup penetration testing & recovery proof: tests backups the way an attacker would
Stork365	Microsoft 365 backup & restore: Exchange, OneDrive, SharePoint, Teams, Entra ID (this document)
ZeroVault	S3-compatible storage for immutable Veeam backups

Who is it for?

- IT and messaging teams responsible for Microsoft 365 data protection and recovery
- MSPs and service providers managing multi-tenant Microsoft 365 environments
- Security and risk teams enforcing an independent, encrypted backup copy
- Organizations with data-residency or sovereignty requirements (bring your own storage)
- Teams with GDPR / KVKK / DORA / ISO 27001 obligations for business data

2. Workload Coverage Catalog

Every Microsoft 365 workload is backed up with its own semantics and its own restore path:

Workload	What is protected	Restore
Exchange Online	Mail, calendar, contacts and tasks for primary and shared mailboxes; full MIME fidelity with delta sync.	Item- or mailbox-level restore to the original or an alternative mailbox; EML/ZIP export; preview before commit; non-destructive by default.
OneDrive	Drive hierarchy, files, folders, version history and permissions / ACLs.	Point-in-time restore and ACL recovery; <i>restore-only-if-hash-differs</i> mode for surgical ransomware recovery.
SharePoint Online	Document libraries and list-backed structured content, including custom column values.	Metadata-preserving restore to the original or an alternative site; hash-based differential recovery.
Microsoft Teams	Standard, private and shared channels plus 1:1 and group chats.	Restored as structured export bundles (JSON with manifests); no live channel replay (a Graph API limit we state honestly).
Entra ID	Users, groups, applications and service principals with membership and ownership.	Three paths: soft-delete recovery (30 days), full object recreation, or property replay via PATCH; group membership add-only.

3. Deployment & Storage

Connection	Microsoft Graph with modern authentication and an app registration; no legacy APIs.
Deployment	Containerized SaaS platform with a web console; no backup infrastructure to run yourself.
Storage (BYOS)	AWS S3, Cloudflare R2, Azure Blob, Google Cloud Storage, SFTP, WebDAV, or local filesystem.
Encryption	Encrypted payload written through Kopia; encryption keys stay under your control.
Scheduling	Automated scheduled backups with delta-first incremental sync.
Cloud scope	Global commercial Microsoft 365 and Entra ID. GCC, GCC High, DoD and 21Vianet are not in launch scope.

Your data, your storage. Backups are written to storage accounts you own, never a vendor-locked repository. Because the encryption keys stay with you, a copy of your Microsoft 365 data never has to leave your jurisdiction.

4. Key Features

- Bring your own storage: S3, R2, Azure Blob, GCS, SFTP, WebDAV
- Workload-aware restore semantics per service
- Delta-first incremental sync
- Item-level and bulk restore
- Preview before every restore
- Ransomware hash-differential recovery (OneDrive & SharePoint)
- Non-destructive restores by default
- RBAC, SSO (SAML / OIDC) and MFA
- Audit logging and SIEM export
- Separation of duties and just-in-time restore access

5. What You Get

- 1 A connected Microsoft 365 tenant with scheduled, workload-aware backups
- 2 Encrypted backup copies in storage you own and control (BYOS)
- 3 A restore explorer to browse, search, preview and recover by workload
- 4 Ransomware-aware differential recovery for OneDrive and SharePoint
- 5 Three-path identity recovery for Entra ID objects
- 6 Access control, audit logging and SIEM export for governance

6. Security & Compliance

Framework	How Stork365 helps
GDPR	An independent, encrypted copy with a clear right to restore; data stays in storage you control.
KVKK	Data residency through bring-your-own-storage, with access logging and role separation.
DORA	ICT resilience: recoverable, independent backups of critical Microsoft 365 data.
ISO 27001	Access control, encryption and audit logging aligned to Annex A controls.
SOC 2	Security, availability and confidentiality controls across backup and restore.

7. Next Step

Start a Stork365 trial. Connect your tenant, choose your storage, and watch your first backup run. Stork365 protects what Microsoft's native retention doesn't.
www.backupsec.com · info@backupsec.com · BackupSec