Terms and Conditions

Endpoint Backup & Recovery - Schedule CB-1

Effective Date: October 14, 2025 | Supersedes prior versions.

Service Summary
Service Provider shall provide Endpoint Backup services ("Endpoint Backup") for Covered Endpoints, defined as workstations, laptops, and servers designated by Client and accepted by Service Provider. Endpoint Backup provides file-level or image-level backup (as configured) to a managed backup platform with restoration upon request, subject to platform capabilities, configured scope, and retention.

Scope of Services
- Agent Deployment & Management. Install, configure, and manage backup agents on Covered Endpoints.
- Workstations (VIP Model). By default, workstation/laptop backups apply to VIP Users identified by Service Provider and approved by Client. Additional VIP designations may be requested in writing and may incur additional fees. Unless otherwise agreed in writing, VIP Users are capped at up to 20% of total endpoints.
- Servers. Server backups may be configured as image-level and/or file-level per Service Provider's standard practices and platform capabilities.
- Monitoring & Remediation. Monitor backup job success/failure and take commercially reasonable steps to remediate failures.
- Restores. Perform data restorations on request, limited to available restore points and configured scope.
- Policy Administration. Manage backup policies (inclusions/exclusions, schedules, retention) consistent with Service Provider's standard backup policy, updated from time to time with written notice to Client.

Backup Frequency & Retention
- Frequency. Backups are performed on an automated schedule (typically nightly) for endpoints with backup enabled.
- Policy-Based Retention. Retention is governed by Service Provider's standard backup policy, which may be updated from time to time with written notice to Client.
- Current Standard (for reference). As of the Effective Date, the standard policy provides:
  - Daily backups retained for 30 days
  - Last backup of each week retained for 52 weeks
  - Last backup of each month retained for 36 months
  - Last backup of each year retained for 10 years

These tiers are illustrative of the current standard and may change in alignment with platform capabilities or policy updates.

Storage Allocation, Pooling & Overage Billing
- Baseline Pools. Unless otherwise agreed in writing, baseline pooled allocations are 500 GB per covered workstation/laptop and 1 TB per covered server across Client's environment. Pools are aggregate (pooled across all Covered Endpoints of the same class).
- Measurement. Utilization is determined by the backup platform's reported month-end stored data (or the platform's standard billing metric).
- Overages. Usage above baseline pooled capacity may be billed at then-current Service Provider rates.
- Usage Review. Service Provider may conduct periodic reviews (e.g., quarterly) and (i) recommend plan adjustments and/or (ii) invoice overages for the preceding billing period based on measured usage.
- No Credits for Under-Utilization. Unused pooled capacity does not carry over or create credits.

Terms and Conditions

Endpoint Backup & Recovery - Schedule CB-1

Service Limitations

- Scope of Data. Backup is limited to the file types, paths, applications, and capacities expressly configured and supported by the platform. Certain data types (e.g., large media libraries, PST files, databases) may require specific configuration or a separate solution.
- Device State. Backups require endpoints to be online, powered, and connected to the internet during backup windows.
- Performance & Restores. Restore times depend on data size, bandwidth, and vendor/platform performance. Service Provider targets commercially reasonable timelines but does not guarantee specific restore completion times.
- No BCDR/RPO/RTO Guarantee. Endpoint Backup is not a business continuity or disaster recovery solution and does not establish Recovery Time Objective (RTO) or Recovery Point Objective (RPO) guarantees. BCDR/RPO/RTO commitments require a separate schedule.
- Compliance Retention. Regulatory or legal retention requirements are not provided unless expressly contracted (e.g., legal hold, WORM storage).
- Platform Dependency. Services and capabilities are limited to the backup platform's native features and the telemetry the device exposes.

Exclusions

- Backups of systems, applications, or cloud services not expressly onboarded as Covered Endpoints.
- Unlimited storage or unlimited retention.
- Liability for data outside configured backup sets or excluded by Client policy.
- Forensic recovery, e-discovery, or chain-of-custody services (available separately).
- Any service not expressly included in this Schedule.

Data Handling & Security

- Encryption. Backup data is encrypted in transit and at rest using industry-standard protocols.
- Data Location. Data resides in U.S.-based datacenters unless otherwise agreed in writing.
- Regulatory Scope. HIPAA, SOC 2, NIST 800-171, CMMC, or other frameworks apply only where expressly stated in the Agreement/Schedule(s).

Offboarding & Data Export

- Project Basis. All offboarding/export work is scoped and billed as a separate project, with a minimum fee of $750.
- Media & Shipping. Client is responsible for the cost of any physical media (e.g., external drives, NAS) and shipping/handling.
- Format & Responsibility. Data is exported in a standard format; Service Provider is not responsible for import, ingestion, or reconfiguration into third-party systems. Data is provided "as-is."
- Post-Termination Retention. Backup data will be retained for up to fourteen (14) calendar days after termination unless otherwise agreed in writing, after which it will be deleted per policy.

Client Responsibilities

- Designation & Approvals. Identify Covered Endpoints, VIP Users for workstation backup, and any special data sets to include; approve designations and changes in writing.
- Endpoint Hygiene. Keep devices powered, connected, and on supported OS versions; avoid storing critical data outside configured paths.

Endpoint Backup & Recovery - Schedule CB-1

- Timely Action. Review and respond to backup failure notices or storage advisories; authorize policy adjustments when recommended.
- Data Outside Scope. Client remains responsible for data not designated or excluded by policy.

General Terms

- Endpoint Backup protects only data included in configured backup sets and successfully transmitted to the platform. Service Provider is not responsible for loss of data outside scope or blocked by device, network, or third-party constraints.
- All response times for backup-related incidents are governed by the Service Level Objectives in Schedule A of the Master Service Agreement (with/without Rapid Response as applicable).
- Fees are billed per the Payment Terms of the Master Service Agreement. Vendor pass-through costs (e.g., storage, egress, extended retention) may apply at then-current rates.
- Service Provider may update its standard backup policy (including retention) with written notice to Client; material changes that reduce retention will be effective prospectively.