

# Backup and Data Retention Policy

Understand backup scope, restoration and retention.

## Key points for reference

- Daily backups and seven restore points.
- Infrastructure separate from the primary environment.
- Backups, archives and legal retention are distinct.

Reference summary. The complete clauses below prevail.

## 1. Included backup scope

This policy covers hosting whose order includes backups. It includes website files and databases in the purchased environment; native mailboxes are included when part of that environment. Scope must be identified before purchase without assuming coverage of external platforms.

Workspace, third-party email, customer devices and external storage have their own terms. File-type, size or quantity exclusions must appear in the offer, not emerge during restoration. Regenerable cache and temporary files may be excluded only without compromising data needed for recovery.

## 2. Frequency, restore points and rotation

Backups run daily with seven rotating restore points: a completed new copy replaces the oldest point. This does not mean seven versions per file or recovery at every intermediate time. Restoration must use the timestamps of completed points.

Daily scheduling targets up to 24 hours between copies in normal operation, not zero data loss. Failed, incomplete or inconsistent copies must be investigated and corrected, not represented as healthy without validation. Specific data-loss (RPO) or recovery-time (RTO) objectives require express agreement.

## 3. Backup separation and protection

Included restore points are held on infrastructure separate from primary hosting, not merely a folder on the same disk. Access must be restricted to authorized people and systems with protected credentials and traceable administrative actions.

Separation reduces exposure to primary-environment failures without eliminating every risk or

replacing a customer-controlled copy. Geographic redundancy, immutability, permanent retention and specific certification are not implied unless expressly included.

#### **4. Requesting and authorizing restoration**

Use authenticated support and identify the service, affected data, desired point, reason and later changes. Scope must be confirmed before overwriting: files, databases and messages may have different timestamps. The requester must be authorized.

Restoration may replace later changes. Where feasible, preserve the current state and test separately. Covered restoration does not incur an undisclosed fee; extraordinary work requires an accepted quotation. Timing depends on volume and complexity without an instant-recovery promise.

#### **5. Integrity and customer cooperation**

Keep independent copies outside hosting and primary credentials, especially before changes. Test files and database recovery: possessing a backup does not establish integrity. Customer-encrypted data depends on customer keys, which must not be submitted through public forms.

A copy may preserve existing corruption or malware. Restoring does not audit or clean the whole application. Liability follows causes and duties; recommending independent copies does not remove Zovvi responsibility for its contracted backup routine.

#### **6. Suspension, closure and deletion**

Suspending access is not deletion. During overdue-payment retention, coverage and technical restrictions must be discussed with the customer. Request export and confirm deletion scope before closure. Do not rely on points already rotated out.

After primary-environment deletion, residual points may remain isolated until completing their seven-day rotation, without reuse for service and subject to legal preservation restrictions. Residual copies do not guarantee reactivation; later payment does not recreate data. Valid duties may require separate restricted preservation.

#### **7. Legal retention is not website archiving**

Tax documents, contract evidence, security and legally retained access logs have separate purposes and periods under the Privacy Policy and law. Retaining those records does not retain customer files, databases or messages for the same period.

Backups are not permanent historical archives or forensic recovery. Personal-data and authority

requests require authority checks and minimization. Material coverage, frequency or retention changes must be notified without retrospectively reducing the purchased service.

