Backup Policy - External

Date	Name	Role	Change	Version
Fri Jan 16 2026	Tim Murnaghan	CTO	Approved	V1.0

Backup Policy

General

All our support system are from cloud Saas providers.

Our production system is on the Cloud Platform. Backups are managed by us via the cloud platform backup system.

Roles and Responsibilities

Responsibility to follow this policy applies to all Integrum ESG employees by storing data in the cloud systems of record. The CISO is responsible for developing, maintaining, and implementing the Backup Policy.

The roles and responsibilities of employees at Integrum ESG are set out in the Roles and Responsibility Policy.

Purpose and Scope

This policy defines the process and procedure for the backup of Integrum ESG’s information and to all systems used to collect, store, process, or transfer information. Cloud backups of Integrum ESG backup processes are in scope for this process/procedure.

Integrum ESG retains the right of ownership over all company-operated networks, systems, and their related data. Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of Integrum ESG are not private and may be accessed by Integrum ESG information technology employees at any time without the knowledge or consent of the user or owner.

Method

- All user-level and system-level information maintained by Integrum ESG must be backed up periodically with Cloud Platform.
- Production database backup is encrypted with the customer managed database encryption key.
- Backups must be performed in a manner to support the information Recovery Point Objective (RPO) & Recovery Time Objective (RTO).
- A backup restore must be performed periodically to validate the defined RPO and RTO. We do this periodically by restoring the production database into a different environment.
- In the Cloud Platform system, the only thing we can do with the backup is to restore or delete it. We cannot modify the backup data.
- Daily immutable backups are saved in the cloud, which will provide the primary fallback option in the case of a crisis for the Integrum ESG's systems.
- Backups must be tested in a restore drill at least yearly. The physical security of backups should be managed by the Cloud Paltform.
- Backups are managed in the cloud platform, which has complete control of all processes via a single management console.

The backup schedule for servers and databases is as follows:

- Full daily backups.
- Backups are performed automatically based on a time interval.
- Backups are stored in a secure and restricted area in cloud services in different region/availability zones.

This policy is subject to change, per review by information technology leadership. Additionally, the policy will be reviewed annually for changes coinciding with information technology environment changes at the Integrum ESG.

Backup Retention method:

- **Daily Backup:** Daily backup should be kept for 21 Days.

Data Restoration:

- Backup effectiveness must be tested periodically.

- As part of the process, we will periodically check to ensure that data can be restored from backup as required.

Document Ownership

The CISO is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with Integrum ESG's review requirements. A current version of this document is available to all members of staff in the company shared platform (Sharepoint).