# Backup Policy

*AlgebraKiT B.V.*
Version 0.1 - June 2019

# Definitions

- **Account Data:** Customer accounts, including access keys, user accounts, and configuration data.
- **Authorised Users:** (i) employees and independent contractors of the Customer who access the Services and the Documentation; and (ii) students and teachers who are authorised by the Customer to use the Services and the Documentation.
- **Authoring Services.** Apply to Authorised Users, being employees and independent contractors of Customer, and include the functionality that allows authors to define, change and publish Exercises using the AlgebraKiT Content Management System and/or the AlgebraKiT API
- **Services**. The Student Services and the Authoring Services.
- **Session Data**. Data generated by the Supplier using the Student Services and relating to Authorised Users in connection with use by Authorised Users of the Software on the Customer Websites, including unique customer identification codes
- **Student Services.** The subscription services to the Software integrated in and accessible via the digital learning environment of Customer provided by the Supplier to the Authorised Users under this agreement via https://algebrakit.com or any other website notified to the Customer by the Supplier from time to time, as more particularly described in the Documentation
- **Exercise Data.** Part of the Customer Data. The data inputted by the Customer or Authorised Users for the purpose of using the Services or facilitating the Customer's use of the Services

# Introduction

This backup policy describes the measures taken by AlgebraKiT B.V. (“AlgebraKiT”, “us” or “we”) to guarantee business continuity in the area of data management. This policy describes which information is safeguarded and what processes are in place to verify the supporting procedures for safeguarding the information.

## Roles and Responsibilities

AlgebraKiT implements the following three roles:

- **Data Officer**: responsible for the overall data management/warehousing in the company.
- **Security Officer**: responsible for the overall IT security within the company.
- **Manager Operations**: plans, coordinates and manages the testing procedures and verifies whether the policies and procedures are implemented correctly.

These three roles work together to make sure the policies and procedures are implemented and followed.

- The *manager operations* will ensure the required facilities are available.
- The *security officer* will ensure safety measures with respect to data and back-up media.
- The *security officer* will ensure access control measures required for safeguarding the data.
- The *data officer* will ensure backup operators are available, check the backup log for completion, be responsible for the safekeeping and availability of all back-up media and logs, and coordinate actual/test restores.
- The *data officer* will ensure backup logs are completed and (if applicable) signed in a timely manner, report any backup failures and logging failures with the *manager operations*, and investigate any reported exceptions.

## Scope

The scope of this backup policy includes the activities performed by AlgebraKiT to:

- safeguard the information assets of AlgebraKiT.
- prevent the loss of data in the case of accidental deletion or corruption of data, system failure, or disaster.
- permit timely restoration of information and business processes, should such events occur.
- manage and secure backup and restoration processes and the media employed in the process.

This policy, and supporting procedures, encompasses all system resources and supporting assets that are owned, operated, maintained, and controlled by AlgebraKiT as part of the **Services.**
**Note**: the (system) backups are not meant for the following purposes:

- Archiving data for future reference.
- Maintaining a versioned history of data.

## Data retention periods

The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of the information.

| **Type of data** | **Backup Frequency** | **Retention Period** |
|---|---|---|
| **Exercise Data** | Daily | 7 Days |
| | Weekly | 1 Year |
| **Session Data** | Daily | 1 Month |

| | | |
|---|---|---|
| **Account Data** | Daily | 1 Month |

Client-specific agreed deviations on this policy are included in the clients' SLA.

# Disposal of Media

Prior to retirement and disposal, it is ensured that:

- The media no longer contains active backup images;
- The media's current or former contents cannot be read or recovered by an unauthorised party.

All backup media will be physically destroyed prior to disposal.

# Verification

On a biweekly basis, logged information generated from each backup job will be reviewed for the following purposes:

- To check for and correct errors.
- To monitor the duration of the backup job.
- To optimise backup performance where required.

The *Data Officer* will identify problems and take corrective action to reduce any risks associated with failed backups.

To verify that backups have been successful, and that the recovery procedures in place are complete, random test restores will be done once every two months.

# Data Recovery

In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 working days if the destroyed equipment has been replaced by that time.

In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.

# Restoration Requests

In the event of accidental deletion or corruption of information, requests for restoration of information will be made to the Manager Operations of AlgebraKiT. Specific contact details can be found in the clients' SLA.