

Spectades HxGN EAM Cloud Services

Data Access Policy

1. Overview and Definitions

The purpose of this Data Access Policy document is to set the data access policies for Cloud Services including supported data access mechanisms, data backup policies, data retention policies, and disaster recovery expectations. Defined terms not explicitly defined herein shall be as defined in the Spectades HxGN EAM Cloud Services Agreement.

“Target” means a desired goal. Targets are not commitments.

2. Supported Data Access Mechanisms

All Customer access to data in Cloud Services is provided via three mechanisms:

- The native functionality of the Software Products running in Cloud Services (e.g. build-in reporting functionality, etc).
- The file Import / Export capabilities built into the Cloud Services.
- Remote application programming interfaces (e.g. REST APIs) built into various Software Products running in Cloud Services.

No other data access mechanisms are supported in Cloud Services including (but not limited to) direct access to the databases underpinning Software Products.

3. Data Backup Policies

All application data for the Software Products running in Cloud Services is backed up on a daily basis. These backups include all databases associated with the applicable Software Products running in Cloud Services as well as any user uploaded files stored in Cloud Services, being Customer Data. Backups are encrypted using industrystandard encryption technology and are stored in a storage subsystem separate from the production storage subsystem.

4. Data Retention Policies

Data backups of Production Customer Environments are retained for a period of thirty-one (31) days.

Data backups of Non-Production Customer Environments are retained for a period of three (3) days.

5. Disaster Recovery

For the Production Customer Environments, the Recovery Time Objective (RTO) Target is 48 hours and Recovery Point Objective (RPO) Target is 24 hours.