Service Level Agreement

Archive-IT - SaaS

Date	**03-09-2025**
Version	**1.5**

secure yesterday,
empower tomorrow.

Table of contents

Version history

Author	Version	Date	Adjustments
Roy Peeters	Concept	02-07-2018	
Hein Boots	1.0	09-05-2019	Adjustments following mutual agreement
Roy Peeters	1.1	26-03-2021	Adjustments deliverables
Roy Peeters	1.2	30-11-2021	Minor textual changes
Roy Peeters	1.3	04-03-2022	Opening hours adjusted
Hein Boots	1.4	18-7-2024	Update several points
Marketing	1.5	03-09-2025	New lay-out

1. General

1.1 Introduction

This Service Level Agreement (SLA) details/explains Archive-IT's service levels in relation to SaaS software.

1.2 Terms and definitions

Capitalised terms used in this SLA shall have the meaning set out in the glossary below, or, if not set out below, the meaning given to them in one of the other parts of the Agreement:

Term	Definition
Support Department	The Support department of Archive-IT.
Management	The proactive, reactive and adaptive management of the SaaS service aimed at its availability and continuity. Including the implementation of patches, new releases and new versions of the underlying applications and system software.
Availability	The SaaS service availability standard is shown as a percentage of the time that, during the Service Window, the SaaS service can be used. Formula: [(Service Window – Downtime)/ Service (Window)] X 100% Availability means the technical possibility of being able to log in to Archive-IT's portal providing access to the SaaS service and providing the agreed functionality.
Change	A change/modification of (a part of) the SAAS service.
Change Advisory Board (CAB)	Those responsible for approving RFCs requests.
Change Manager	Final responsible of Change Advisory Board.
Downtime	Period that the SaaS service is unavailable within the Service Window.
Incident	Operational event that is not part of the standard operation of the SaaS service and results in a degradation of the agreed operational service.
Notification	General questions, requests and complaints, not being an Incident.

Maintenance	Performing corrective, adaptive or preventive maintenance work. This includes regular updates of environment and software (firewall updates, security patches, operating system, etc.), among others.
Maintenance window	The period in which Archive-IT (a) performs scheduled maintenance work; and (b) performs necessary extra maintenance for which no delay is possible (think security risks etc.).
Resolution time	The number of working hours between the time of handling an Incident and the resolution of the Incident.
Patch of Fix	A modification to the underlying application(s) or system software to fix errors.
Problem	An undesirable situation identified from related Incidents, the cause of which is not yet known.
Response time	The time elapsing between the notification of the Incident by the Client in accordance with the agreed reporting method and the moment the notification is dealt with by Archive-IT.
RFC – Request for Change	An RFC is synonymous with a Change Ticket. A request to change (a component of) the SaaS service.
Service Window	Period during which the SaaS service takes place minus the maintenance window.
Working days	Monday to Friday excluding national (Dutch) recognised holidays (as indicated on the central government website).
Working hours	From 08:15 to 17:00 on weekdays.
Workaround	A temporary solution to an Incident.

2. Software

2.1 Submission of incidents/reports

For Incidents/Reports relating to Archive-IT software, please contact the Support Department via the secure online support portal. Incidents/reports can be registered 24/7. You can also view the progress and history of your Incidents/Reports in this online support portal.

Do you not yet have access to this? Then you can request this via support@archive-it.group.

2.1.1 Support desk availability

The Support Department monitors the progress and feedback of Incidents/Reports. The Support Department can be reached on regular working days between 8.15 and 17.00. There is no staffing on weekends and public holidays.

In case of high urgency/emergency, an Incident can also be reported/clarified by telephone (on regular working days/working hours). The Support Department can be reached via telephone number +31 77 750 11 00.

Archive-IT will make every effort to resolve Incidents within the set Resolution Time (see chapter response and resolution times).

2.1.2 Incident management

The following steps are followed upon receipt of an Incident/Notification:

- Classification and prioritisation.
- Monitoring on progress until final sign-off.
- Communication of status information.
- Handling of Incidents/Reports.

An Incident may lead to a Request For Change (RFC).
Incidents/Notifications may lead to an RFC. The Incident/Notification will thereby be temporarily put on hold - with a reference to the RFC. In case of high urgency, it may be decided to propose a Workaround or Fix within the set Resolution Time.

Retention period for attachments and screenshots
Attachments and screenshots in support tickets are retained for one year. During this period, these files can be accessed, including in closed tickets. When a ticket has been

closed for more than one year, all attachments and screenshots are removed from the ticket and are no longer accessible. This prevents sensitive information from being stored longer than necessary.

2.1.3 Response and resolution times

Response and resolution times are defined based on the specified impact and classification. The combination of these determines the priority.

Establish impact code

Impact code	Scope of the Incident
High	More than 10 users or business critical processes
Middle	2-10 users
Low	1 user

Vaststellen incident classificatie

Impact code	Consequence of the Incident
High	Continuing work is not possible or it affects business critical processes
Middle	Continuing work is difficult
Low	Continuing work is possible

Prioritisation

The combination of **impact code** and **classification** determine the priority of an Incident.

Priority Classification			
Impact code	**High** **(Continuing work is not possible)**	**Middle** **(Continuing work is difficult)**	**Low** **(Continuing work is possible)**
High (> 10 users)	I	I	II
Middle (2-10 users)	I	II	III
Low (1 user)	III	III	III

Urgency determination

Depending on the priority, urgency will be determined, according to the matrix below.

Resolution and response time		
Priority	**Response time**	**Resolution time**
I (urgent)	< 1 working day	< 1 working day
II (less urgent)	< 1 working day	< 1 workweek

III (not urgent)	< 1 working day	< 1 month

Archive-IT shall also, if the cause of the Incident is not attributable to Archive-IT, make every effort to resolve Incidents. Archive-IT does not, however, apply 'Resolution Times' for such Incidents. Archive-IT is entitled to charge a fee for the work performed in this context at its usual rates.

2.1.4 Incident/reporting reports

Through the online support portal, you can report the following issues:

- Number of Incidents.
- Per Incident the 'Resolution Time' and 'Response Time'.
- The number of Incidents grouped by priority..
- A list of open Incidents and RFCs.

2.2 Scheduled maintenance

Scheduled maintenance for the SaaS service takes place outside working hours/working days during the maintenance window.

Maintenance at Operating System and infrastructure level

This concerns (security) updates at OS level (Windows updates) and possible maintenance at infrastructure level, which is carried out by our hosting partner. One week before the release in the production environments, Archive-IT first tests this maintenance extensively in the acceptance environment. If (expected) problems are found, the roll-out in the Archive-IT production environments will be postponed.

Normally, this maintenance takes place on Wednesday evening/night between 20:00 and 01:00. About 13 maintenance occasions per year are designated, which are notified at least 4 working days in advance.

Archive-IT software maintenance

During regular Archive-IT software maintenance, the availability of the software is not at risk (unless in exceptional cases, in which case Archive-IT will report this immediately), because the SaaS architecture of Archive-IT software and the umbrella rollout mechanism take into account a rollout without availability consequences. Should a problem nevertheless occur, it is easy to revert to a previous version within a short period of time.

This maintenance takes place - as required or necessary - outside working hours and is notified at least 4 working days in advance.

2.3 Change and Release Management

Requests for changes to the software should also be made in the online support portal. Archive-IT will assess the proposed change for feasibility and consequences (including costs) and determine if/to what extent the proposed change will be implemented. A change request that is not approved will be rejected by Archive-IT with reasons.

Release Notes will be prepared for important updates.

2.4 Escrow software

Parties value continuity, as far as software and hosted data are concerned. Archive-IT is the right address for this. If you want even more security: Archive-IT has found a reliable party that can provide a solid Escrow facility. If you are interested, please contact Archive-IT for further details on Escrow.

2.5 Service parameters SaaS

2.5.1 Availability

The SaaS service is made available within a platform of Infrastructure-as-a-Service services and offered with an availability guarantee* of 99.9%. This is done in cooperation with the data centre partner from data centres in the Netherlands.

* In this context, **unavailability** means unavailability for all users (complete unavailability).

The underlying infrastructure meets heavy security requirements, high availability and redundancy of all primary facilities. All data and its backup are redundantly stored at two different locations in the Netherlands.

Infrastructure management focuses on keeping the managed servers and related infrastructure components available and up-to-date. To this end, the following activities can be defined:

- Server Management.
- Security.
- Monitoring.
- Back-up.

2.5.2 Regular maintenance

Regular maintenance means performing corrective, adaptive or preventive maintenance activities. This includes regular updates of environment and software (firewall updates, security patches, operating system, etc.).

2.5.3 Application Services

Application services take care of all activities related to delivering applications to end users. Application services concern the provision of application-oriented services to users and include planning, executing and controlling the daily management tasks. It also ensures optimal operation of one or more applications so that the desired information system functionality is available to users at all times.
The following services are concerned:

- Monitoring: monitoring application availability by monitoring 'key application events'.
- Patch Management: applying patches, updates and new versions of application software.
- Back-up & restore data.
- Security services.
- Manage resources at the application level.

2.5.4 Datacenter services

Datacenter services provides operational management, maintenance and operation of the hosted server configurations in the data centre, including the associated Operating Systems (OS), other control software products and peripherals. The services are:

- Monitoring: monitoring the availability and reliability of server configurations of servers placed in the Data Centre.
- Incident Management: handling failures with server configuration(s) according to the Incident Management process.
- Preventive Maintenance to Prevent Incidents.
- Patch Management: applying patches and updates to OS and non-application related software products.
- Documentation.

2.5.5 Back-up and restore services

Backup and restore services preventively create copies of the data present. This secures the data in case the data in the original location is lost or damaged. If necessary, a backup can be restored to its original location. The following activities are performed:

- Monitoring: monitoring whether the backup was successful or not.
- Performing back-ups.
- Performing restores.
- Check: performing a periodic backup check.

RPO: A full backup is performed weekly. A backup of SQL transaction logs is also performed every 30 minutes. This limits the maximum data loss for successful backups to 30 minutes. Backups are kept for one month.

Restore requests

Archive-IT will initiate a restore request within 2 working hours of receiving it. The RPO (date and time to be restored to) of the restore request must be specified by the Client and can be up to one month back. RTO (lead time of a restore) depends on the amount of data. During a restore, the Virtual Archive environment is not accessible.

Restore and backup controls

At least once a year, database restore tests take place at the hosting centre to check the restore process. Where necessary, improvement actions are taken.
The back-up process is also checked and remedial action is taken where necessary.

2.5.6 Security services

The security policy is embedded in all Archive-IT services. Regular audits are performed to check whether services are carried out in accordance with the security guidelines. Furthermore, the security guidelines and procedures are available to every Archive-IT employee.

Servers and Storage

The data centre used by Archive-IT meets general physical security requirements, such as access controls, power supply, fire safety, etc. The infrastructure is monitored 24 hours a day, 7 days a week, 365 days a year. Various preventive protection measures are also in place, such as firewall management, standard antivirus and patch management.

Network

The network is the foundation for secure applications and information flows, and therefore secure business processes. Especially the integration of security measures provides benefits. The network components must provide security themselves and cooperate intensively with the various security solutions (security solutions) without making the infrastructure too rigid..

Firewall Services

The purpose of a firewall in a computer network/or on a computer is to prevent unwanted traffic from one network zone from entering another, in order to increase security in the latter. The protected network is often an intranet or internal network, and this is protected from the Internet. The unwanted traffic consists, for example, of attacks by hackers and crackers (crackers), computer viruses, spyware and denial of service attacks.

Firewall services provides the set-up and operational management of a firewall, including a single dmz (demilitarised zone) interface.

The following activities will be carried out:

- Monitoring: monitoring the availability of the Firewall configurations.
- Firewall management: ensuring operational management of the Firewall configurations including the associated control system.
- Preventive maintenance to prevent Incidents.
- Documentation: Documenting the Firewall configurations, system software and procedures.

3. Exit and retransition plan

3.1 Scope

At the end of the agreement, transfer of data may take place from Archive-IT to client or third party. The transfer of data during exit and retransition is done on the basis of the management situation 'as-is'. The existing services continue during the exit and retransition on the basis of the existing agreements in the agreement.

If the exit and retransition activities are not completed after the end of the agreement, these activities will be continued by Archive-IT - at agreed costs - until final discharge by the client. Regular changes to the existing services during the exit and retransition will therefore take place within those agreements and do not fall within the scope of this exit and retransition plan.

Infrastructure changes as a result of the transfer will be made through the standard change procedures in place at that time. Where necessary, the start of the change is preceded by a substantive alignment of the parties' technical specialists.

3.2 Continuity

Client will be inconvenienced as little as possible by the contract termination and exit and retransition. The parties commit to working together during the exit and retransition process. Archive-IT is responsible for ensuring that the agreed service levels are maintained.

3.3 Organisation

For the purpose of implementing exit and retransition, the parties will each appoint an exit and retransition manager. The exit and retransition managers are the point of contact for each party and are given sufficient mandate to fulfil the agreed arrangements in this exit and retransition plan. With regard to the scope of the mandate, internal mandating, governance rules and restrictions should be taken into account. The implementation of this exit and retransition plan will be tackled energetically. The parties will coordinate schedules to the best of their ability in order to make the exit and retransition take place as quickly as possible. Archive-IT will make sufficient and well-qualified staff and other resources available for the implementation of a controlled exit and retransition.

3.4 Acceptance, discharge

Discharge takes place upon acceptance of transfer of the relevant services by the Client.

Upon discharge, there may be residual items. After discharge, Parties look at which residual items are still outstanding and need to be finished.

3.5 Activities and deliverables

The activities performed by Archive-IT in the context of the exit and retransition must be delivered by Archive-IT, as well as the deliverables. In any event, a secure and transparent data export must take place on a data carrier that is readable and secure for the Client at that time.

Archive-IT shall cooperate in making available answers to questions asked within agreed deadlines (questions from Client and/or third parties involved in the transfer). If the Client does not find the deadlines reasonable and is bothered by this, a new deadline must be agreed by the parties. Archive-IT's provisions with regard to data and information security shall be maintained until the data and any other information have been transferred. Archive-IT will not suspend its obligations under this exit and retransition plan if a conflict arises over the termination of the cooperation.

3.6 Deliverables Archive-IT

The following deliverables apply:

- Make analysis of exports and coordinate with client..
- Record or determine:
  - In what format the data and metadata should be provided.
  - Whether the history of the files should be included.
  - Whether versions of the electronic documents should be included.
- Figuring out further questions, such as:
  - How many export runs should we perform (test runs and production run)?
  - How often do we need to deliver the data and how?

Archive-IT will complete and work out an analysis within four weeks of the exit request. Archive-IT will start creating the export service within two weeks after the order.

3.7 Confidential information

The parties will respect each other's interests, intellectual property and confidentiality of information.
Archive-IT's duty of confidentiality will continue to exist indefinitely after the exit and retransition.

3.8 Costs exit/transition

Archive-IT shall ensure that upon termination of the agreement the exit and retransition activities and deliverables are carried out or delivered as described in this document. The costs related to the exit and retransition regarding the digital/physical data are for the account of the Client. Before carrying out an exit or transition project, Archive-IT will make an offer.

4. KPI's SaaS software

Nr.	KPI	Description	Norm	Explanation
1	Availability	Availability of the SaaS environment	99,9%	Measured within service window 24/7, excluding scheduled maintenance.
2	Security management	Keeping antivirus software up to date	100% < 36 hours after updates are released	After a virus/antispam update comes out for the virus scanner, it is rolled out on the relevant systems.
3	Security management	Implementation of critical security updates	100% < 72 hours	Archive-IT ensures most recent security updates are in place.
4	Backup	Perform backup and restore	Continuously every 30 minutes	Daily backup of client data stored within the hosted environment.
5	Restore	Maximum data loss	30 minutes	The maximum amount of time in which added or changed data may be lost. Applies to all production data.
6	Performance Virtual Archive	An image is available within five secondS	90% of retrieved images are available within the five-second time limit	The definition is that the overview of scanned files is on the screen within five seconds. Clicking a specific file afterwards is also within five seconds. E.g. assuming optimal available bandwidth of the Internet.