

Service Level Agreement

Self-service bag drop



Part of the agreement "Self Service Bag Drop at Eindhoven Airport NV"

Table of contents	
Article 1 General	3
Article 2 Definitions	3
Article 3 Service description	4
Article 4 Availability	5
Article 5 Incident management and support	5
Article 6 Continuity management	6
Article 7 Change management and maintenance	7
Article 8 Monitoring and alerting	7
Article 9 Security and patch management	7
Article 10 Reports	8

Article 1 General

- 1.1.1 This Service Level Agreement (SLA) is applicable for service and maintenance, as agreed in contract “Self Service Bag Drop at Eindhoven Airport NV” (hereinafter: “Agreement”) and gives a survey of the quality agreement made between Supplier and Client.

Article 2 Definitions

- 2.1 In this SLA, the following definitions are used in addition to the definitions defined in the Agreement,
article 1 of the General Provisions,
article 2 of the Special Provisions Housing and Hosting,
article 2 of the Special Provisions Professional Services,
article 2 of the Special Provisions SaaS,
article 2 of the Special Provisions Software,
of the General Purchase Conditions IT & Systems (GPCITS).

UAT-system	An environment identical to the System, intended to test and validate functional and technical changes, in order to avoid incidents in the System
GPCITS	General Purchase Conditions IT & Systems
Availability	The percentage of the time the system functions according to the required specifications.
Downtime	The time the System is not available conforming the required specifications.
Effective Downtime	All Unplanned Downtime not occurring in Maintenance Window, with exception of Unplanned downtime due to force majeure.
Planned Downtime	Downtime, occurring during the Maintenance Window or priorly approved by EANV.
Unplanned Downtime	Downtime due to a failure of Downtime not timely announced to EANV.
Resolve time	Time between the moment EANV reports the failure to Supplier and the time Supplier has resolved the failure and reports so to EANV.
Response time	The time between the moment EANV reports the failure to Supplier and the moment Supplier starts to resolve the failure.

Service Window	The time window in which Supplier is supposed to work on a solution to an incident of failure or service request.
System	The total of software and hardware provided by Supplier on behalf of the contract.
Uptime	Synonym for Availability.

Article 3 Service description

- 3.1 The Service contains maintenance and support of the System.
- 3.2 All costs resulting from this SLA are included in the Agreement as described in article 5. No additional costs can be charged at EANV.
- 3.3 Scope of Service delivery

The scope of the service delivery will include:

- Second line and third line of preventive and corrective maintenance (first line will be scope of EANV)
- All parts needed for preventive and corrective maintenance for complete contract period with a maximum of € 500,- per part have be included in the service delivery price.
- Providing a part list with prices of all parts of the unit
- Providing an maintenance plan for replacement of parts (end of life) for the complete contract period
- All software updates for the complete contract period

Article 4 Availability

4.1 The System is considered to be having Downtime, when more than 2 SSBD units are not working as required.

4.2 Availability will be calculated per calendar month with the following formula:

$$\text{Availability} = \frac{\text{number of minutes in calender month} - \text{Effective Downtime}}{\text{Number of minutes in calender month}} * 100\%$$

Example

Month: December 2022. This month contains 44640 minutes (31 days * 24 hours * 60 minutes).

Planned Downtime: 30 minutes

Unplanned Downtime: 240 minutes, from which 20 minutes by force majeure.

The Availability that month is: $\frac{44640 - (240 - 20)}{44640} * 100\% = 99,51\%$

4.3 Supplier guarantees an Availability of 99% (ninety nine percent).

4.4 In case it appears from analysis Unplanned Downtime is caused by force majeure, as described in Article 16 of the GPCITS – General Provisions, this Downtime will be marked as force majeure.

Article 5 Incident management and support

5.1 Incidents and support requests will be classified as follows:

Priority	Description
Critical	4 or more SSBD units are not working as required
High	2 or more SSBD units are not working as required
Medium	1 SSBD unit is not working as required
Low	A support request

5.2 In case of an incident or support request Supplier will respond as follows:

Priority	Maximum response time	Maximum resolve time	Service Window
Critical	< 1 hour	< 2 hours	Calendar days 04:30 – 23:59
High	< 4 hours	< 8 hours	Calendar days 04:30 – 21:00
Medium	< 1 day	< 3 days	Working days 09:00 – 17:00
Low	< 2 days	< 5 days	Working days 09:00 – 17:00

Response time and resolve time will be cumulated.

Explained in the following examples:

Example 1: a critical incident is reported on 04:30 on any day, the incident must be resolved by 07:30 at the same day.

Example 2: a high incident is reported on a Friday at 10:00 the incident must be resolved by 05:30 on Saturday at the latest.

Example 3: a medium incident is reported on a Friday (before 17:00) the total time between the incident reported to supplier and the moment the incident must be resolved is 4 working days. So the incident has to be resolved on the next Thursday 17:00 at the latest.

- 5.3 Supplier has a fixed procedure for reporting and follow up of incidents and support requests. This procedure is equal to all priorities and for all calendar days and time of the day.
- 5.4 EANV has one (1) service point for incidents and support requests regardless of the nature of the incident or support request.
- 5.5 1st line of support (corrective maintenance) will be the technical service of EANV
- 5.6 2nd line of support (corrective maintenance) is allowed to be performed remotely.
- 5.7 3rd line of support (corrective maintenance) will be on-site support.
- 5.8 2nd and 3rd line of support will be available on calendar days from 04:30 – 23:59 (Amsterdam Time zone).
- 5.9 Incidents and support requests can at least be reported by telephone and by email to Supplier. The preference however is the ability to report directly to a web-based portal from Supplier.
- 5.10 Supplier will provide a web-based portal to EANV in which the actual status of incidents and support requests can be monitored.
- 5.11 A support request can lead to a change request as described in Article 7.

Article 6 Continuity management

- 6.1 Supplier will perform a full, non-incremental back-up of the System, at least once every month and after every System update or configuration change.

- 6.2 The back-up shall contain all data of the System, including but not limited to master data, settings, configuration files, licenses, media files and databases.
- 6.3 Supplier will store back-ups for at least six (3) months.
- 6.4 Supplier will store the most recent, validated back-up off-site the premises of EANV.
- 6.5 Supplier has *disaster recovery* procedures and recover manuals in place.
- 6.6 Tenderer will at least quarterly perform a restore of the most recent back-up on the User Acceptance Test system (UAT), in order to validate the back-up and recovery procedure, which has be to be discussed and approved by EANV

Article 7 Change management and maintenance

- 7.1 Supplier is responsible for all maintenance activities (software and hardware) on the SSBD units as prescribed by the manufacturer and warranty terms, except daily or weekly maintenance (1st line of support).
- 7.2 In case maintenance will lead to (possible) Downtime, Supplier will submit a maintenance request to EANV 5 working days prior to the maintenance. EANV will strive for a reply within 2 working days.
- 7.3 Supplier shall validate maintenance activities by applying them to a test system in advance of the actual maintenance.
- 7.4 Supplier will at least perform Preventive Maintenance once a month, in order to detect potential problems and to notice possible failures in an early stage.

Article 8 Monitoring and alerting

- 8.1 EANV is responsible for adequately monitoring the SSBD units with the goal to detect failures, wrong use, and potential incidents in an early stage.
- 8.2 EANV will automatically be alarmed when a failure is detected and the SSBDs are not functioning according to the specifications. This can be achieved for example with a web-based dashboard in which all SSBD units are represented with the current status.

Article 9 Security and patch management

- 9.1 Supplier is responsible for implementing patches, updates and upgrades in a timely and adequate manner.
- 9.2 In case vulnerabilities are known in the (System) Software, Supplier will follow-up on these as soon as possible. To determine the priority, the classification of the Dutch National Cyber Security Centre (NCSC) shall be used, as published on <https://advisories.ncsc.nl/advisories> , with respect to the following table:

Probability	Severity	Incident priority
High	High	High

High	Medium	Medium
Medium	High	Medium
Medium	Medium	Medium
Overig		Low

- 9.3 If no NCSC-classification is known, the vulnerability priority shall be discussed between EANV and Supplier.

Article 10 Reports

- 10.1 Every three (3) months Supplier will report to EANV with regards to the performance of the SSBDs and the performance of Supplier. In the report at least the following subjects on a monthly basis will be covered: Availability, Planned Downtime, Unplanned Downtime, Effective Downtime, incidents (including description, priority, reaction time and response time) and support requests.