

# Schedule 6C

**[Draft version]\***

## Service Level Agreement (SLA)

KB, National Library of the Netherlands

March, 2026

*\*This document is provided as a draft/example by the Contracting Authority to give tenderers insight into the expected operational agreements, working methods and governance arrangements. The Programme of Requirements (PoR) takes precedence and is binding; requirements derived from the PoR are not subject to discussion. Yellow-highlighted sections indicate the Contracting Authority's preferred operational approach and require alignment with the successful Tenderer; these sections are subject to discussion and are not final until formally approved.*

**Signature Contracting Authority:**

**Date:**

**Signature Contractor:**

**Date:**

# Table of Contents

<b>1</b>	<b>General</b>	<b>3</b>
<b>2</b>	<b>Support and Maintenance</b>	<b>5</b>
<b>3</b>	<b>Service Level Agreements</b>	<b>7</b>
<b>4</b>	<b>Service Description &amp; Service Management Practices</b>	<b>9</b>
<b>5</b>	<b>Service Reporting &amp; Continuous Improvement</b>	<b>10</b>
<b>6</b>	<b>Exit</b>	<b>11</b>
<b>7</b>	<b>Schedules</b>	<b>12</b>

## Version Control

Version	Date	Author	Changes
0.1	..	..	Draft version
0.2	..	..	..

Table 1: Version control for the SLA

# 1 General

## 1.1 Purpose

This Service Level Agreement (SLA) sets out the qualitative and quantitative agreements relating to the [application(s)/service(s)] between the Contracting Authority and the Contractor.

This SLA forms part of the Framework Agreement and includes the service levels and performance agreements applicable to the Services. It also ensures compliance with applicable Dutch laws and regulations, including the NIS2 Directive and the Baseline Information Security for Government Baseline (BIO).

In addition to this SLA, a Dossier of Agreements and Procedures (DAP) applies, which elaborates the operational processes, procedures and communication.

## 1.2 Term

- The commencement date of this SLA shall correspond to that of the effective date of the Framework Agreement.
- The duration of the SLA shall correspond to that of the Framework Agreement.

## 1.3 Description of the Services

- The Services shall be delivered in accordance with the requirements set out in the Programme of Requirements (PoR).
- Further specification and scope are included in the Service Catalogue (Chapter 4).

## 1.4 Related Documents

Hierarchy	Document	Owner	Date	Version
1	Framework Agreement incl. Schedules (incl. SLA and Exit Plan)	..	..	..
2	Data Processing Agreement	..	..	..
3	Verification meeting report	..	..	..
4	Second Memorandum of Clarifications	..	..	..
5	Descriptive Document including Schedules	..	..	..
6	ARBIT 2022	..	..	..
7	Other Schedules	..	..	..
8	The Tender submission	..	..	..

Table 2: Related documents and their hierarchy

## 1.5 Document Management

- The Contractor is responsible for maintaining the current version of the SLA.
- Changes to the SLA shall be discussed in the tactical consultation, formally agreed in writing, and recorded in the version control.

- Both Parties shall formally approve changes by signing the updated version.

## 1.6 Evaluation of Service Quality / SLA

- Annual SLA evaluation (formal review).
- At least 2 months prior to the end of the contract period: evaluation and decision on extension or amendment of the SLA.

## 1.7 Signature

- This SLA shall be signed by authorised representatives of both Parties.
- The Contracting Authority shall be represented by a duly authorised signatory.

## 2 Support and Maintenance

### 2.1 Support by Contractor

- The Contractor shall provide a service desk accessible during business hours (09:00–17:00 CET) via telephone, email and/or ticketing system.
- For P1 incidents and security incidents, 24/7 availability shall be provided.

### 2.2 Maintenance and Service Window

- The Services shall be available on a 24/7 basis.
- Maintenance activities shall be performed without impact on agreed availability and performance, in accordance with the PoR.
- Updates, changes and maintenance shall, in principle, be performed **using live deployment methods**, without service interruption, unless this is demonstrably not feasible.
- **Maintenance affecting service availability shall only take place after prior alignment and explicit approval by the Contracting Authority.**
- In the event of urgent security risks or incidents, the Contractor may take immediate measures, informing the Contracting Authority as soon as possible.

### 2.3 Security & Backup

- Patch management shall be performed in accordance with the CVSS classification below:

Type	CVSS Score	Implementation
Critical security patches	≥ 9.0	< 1 week
High security patches	7.0 – 8.9	< 2 weeks
Other patches	< 7.0	Next maintenance window

Table 3: CVSS classification and implementation timelines

- Compliance with patch timelines is mandatory and measurable.
- Multi-factor authentication (MFA) is mandatory for all administrative access.
- Security event logs shall be retained for a minimum of 3 and a maximum of 12 months.
- Continuous monitoring (24/7) of systems and security events shall be in place.
- Backup policy includes at least daily incremental and weekly full backups.
- Recovery Time Objective (RTO): maximum 8 hours.
- Recovery Point Objective (RPO): maximum 24 hours.
- Vulnerability scans shall be performed at least quarterly.
- Security incidents shall be reported within 24 hours.
- A detailed incident report shall be delivered within 72 hours.
- A final report including root cause and remediation shall be delivered after closure.
- Backup and restore processes shall be tested at least annually (see DAP).
- Logs and metrics shall be exportable to the Contracting Authority's monitoring systems (preferably OpenTelemetry, alternatively Prometheus).

### 2.4 Configuration, Change and Version Management

- Changes shall be executed through a controlled and auditable change and release process (further elaborated in the DAP).

- All changes shall be traceable to a change request, incident or release.
- Changes impacting availability, functionality or security shall be communicated in advance.
- The Contractor shall ensure no negative impact on agreed service levels.
- The Contractor shall provide an acceptance environment functionally equivalent to production, supporting end-to-end testing including integrations.

## 2.5 Maintenance

- Planned maintenance shall be announced at least **10 working days** in advance.
- Maintenance shall not result in breaches of agreed availability and performance requirements.
- Urgent maintenance for security risks may be performed immediately, with prompt notification to the Contracting Authority.

### 3 Service Level Agreements

#### 3.1 Prioritisation and Response Times

- Prioritisation shall be determined using an impact and urgency matrix, resulting in priority levels (P1–P5) as defined in this SLA.
- Response and resolution times are binding and measurable.
- Security-related incidents shall be resolved in accordance with Section 2.3.
- At least 95% of incidents shall be resolved within agreed SLA timelines.

Priority Level	Definition
P1	..
P2	..
P3	..
P4	..
P5	..

Table 4: Priority levels and definitions

		Impact		
		Low	Medium	High
Urgency	Low	5	4	3
	Medium	4	3	2
	High	3	2	1

Table 5: Impact and urgency matrix

Priority	Response Time	Resolution Time	Communication	Escalation
P1	15 min	8 hours	Every hour	after 7 hours
P2	1 hour	16 hours	4 hours	after 12 hours
P3	4 hours	5 days	Daily	after 4 days
P4	..	..	..	..
P5	..	..	..	..

Table 6: Response, resolution, communication and escalation times

#### 3.2 Service Level Targets & KPIs

- KPIs are derived from the PoR (Chapter 5A–5F).
- Availability: 99.7% per month.
- Incident handling:  $\geq 90\%$  within response time.
- The solution supports at least 1,000,000 registered users and 50,000 concurrent users.

- 100% of critical vulnerabilities resolved within agreed timelines.
- Quarterly vulnerability scans and annual penetration tests.
- Incident reporting compliant with 24h / 72h / final report requirements.
- Performance: 95% of requests  $\leq$  2 seconds under normal load.
- Scalability: supports 2–3 $\times$  peak load without degradation.
- Backup processes shall not impact availability or performance.

### 3.3 Service Management and Review Processes (SLM)

- Continuous monitoring of SLA performance.
- Monthly reporting including performance, trends and deviations.
- Quarterly review of SLA targets and improvement measures.
- Annual formal evaluation between Parties.

## 4 Service Description & Service Management Practices

### 4.1 Service Description & Service Catalogue

- All Services are described in the Service Catalogue, including scope, responsibilities and service levels.

### 4.2 Service Level Management

- SLA indicators are monitored and reported.
- Deviations are analysed and followed up via the Service Improvement Plan.

### 4.3 Incident and Issue Management

- Incident management complies with this SLA and is operationalised in the DAP.
- Security incidents reported within 24 hours and detailed within 72 hours.
- Root Cause Analysis (RCA) delivered within 5 working days for P1 incidents.

### 4.4 Service Request Management & Service Desk

- Service requests handled within agreed timelines.
- Service desk acts as single point of contact.

### 4.5 Changes and Releases

- Controlled and auditable change and release process.
- Testing in acceptance environment prior to production.
- Test reports delivered for each release.

### 4.6 Monitoring & Event Management

- Continuous monitoring of availability, performance, capacity and security.
- Metrics/logs exportable (OpenTelemetry / Prometheus).

### 4.7 Availability, Capacity & Continuity

- Capacity and performance reviewed periodically.
- Continuity measures aligned with RTO/RPO.

### 4.8 Knowledge Management & Documentation

- Documentation maintained and provided to the Contracting Authority.

### 4.9 Security & Compliance

- Compliance with NIS2, BIO and PoR requirements.
- Annual audits and penetration tests.
- Accessibility compliance with **EN 301 549 and WCAG A/AA.**

### 4.10 Escalation

- Escalation via operational → tactical → strategic levels.
- Roles and procedures defined in the DAP.

## 5 Service Reporting & Continuous Improvement

### 5.1 Reporting

- Operational reporting is provided **periodically**, and security reporting shall be provided quarterly.
- Accessibility reporting shall be provided in accordance with applicable accessibility requirements.
- Test reports shall be provided for each release.

### 5.2 Meeting Structure & Evaluations

- Operational: **bi-weekly or monthly**
- Tactical: **quarterly**
- Strategic: **annually**
- Chain coordination: at least semi-annually

### 5.3 Service Improvement Plan (SIP)

- **Based on analysis, reporting and evaluations.**
- **Improvement measures tracked and evaluated.**

## 6 Exit

### 6.1 Principles

- Exit activities comply with the PoR exit requirements.
- The Contractor shall provide full, timely and active cooperation free of charge.
- Services remain available at agreed service levels during transition unless otherwise agreed.
- Obligations remain in force until formal acceptance of exit.

### 6.2 Acceptance Criteria

- The transition and transfer shall be complete, accurate and usable.
- Data shall be complete, readable and validated for integrity.
- Documentation shall be complete and up to date.
- Access rights shall be correctly transferred or revoked.
- Exit testing shall be successfully completed.
- Data deletion shall be demonstrably completed.
- All transfers shall be logged and validated.
- If the acceptance criteria are not met, the Contractor shall remain responsible for remediation until acceptance is achieved.

## 7 Schedules

### 7.1 Service Catalogue

Service	Description	Features	Users	Availability	Service Hours	KPIs	Dependencies
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..
..	..	..	..	..	..	..	..

Table 7: Response, resolution, communication and escalation times

### 7.2 Rates for Additional Services

- Includes additional service costs, hourly rates, penalties / service credits.

