

MINIMALE INHOUD VAN EEN SLA

Een goed gestructureerde SLA bevat minimaal de volgende onderdelen:

1. Doel en reikwijdte
2. Definities en terminologie
3. Serviceniveaus en KPI's
4. Prioritering en escalatie
5. Monitoring en rapportage
6. Boetes en beloningen
7. Wijzigingsbeheer
8. Feedbackmechanismen
9. Beëindiging en exitstrategie

Toegevoegd in het kader van de Assessments op het SURF normenkader (uitgangsniveau 3): bijlage met betrekking tot specifieke onderdelen aan de SLA in het licht van dit normenkader.

1. Doel en reikwijdte

- Beschrijving van de dienst(en) waarop de SLA van toepassing is.
- Identificatie van betrokken partijen (dienstverlener en afnemer).
- Relatie met de hoofdovereenkomst.

Waarom van belang:

Het definieert de context van de dienstverlening en voorkomt misverstanden over wat wel en niet onder de SLA valt. Dit is cruciaal voor juridische duidelijkheid en operationele afbakening.

Instrumenten:

- Dienstencatalogus
- Scope-documentatie
- Contractuele bijlagen

SURF-relevantie:

Helpt bij het afbakenen van verantwoordelijkheden in ketensamenwerking (ketenbeheer). Duidelijke scope voorkomt risico's bij overdracht van data of diensten.

2. Definities en terminologie

Uitleg van gebruikte termen zoals "uptime", "incident", "respons- en oplostijd", "prioriteit", etc.

Waarom van belang:

Zorgt voor eenduidige interpretatie van SLA-afspraken. Vermijdt verschillende interpretaties bij incidentclassificatie, beschikbaarheid, etc.

Instrumenten:

- SLA-glossarium
- ITIL/ISO-standaarddefinities

SURF-relevantie:

Bevordert consistentie in communicatie over beveiligingsincidenten en compliance-rapportages.

3. Serviceniveaus en KPI's

Dit wordt onderverdeeld in onder andere:

- Beschrijving van meetbare prestaties:
 - Beschikbaarheid (bv. 99,9% uptime).
 - Reactietijd op incidenten (bv. binnen 2 uur voor P1).
 - Oplostijd (bv. binnen 8 uur voor P2).
- SMART-geformuleerde KPI's

Waarom van belang:

Maakt prestaties meetbaar en toetsbaar. Geeft afnemers grip op de kwaliteit van dienstverlening.

Instrumenten:

- SLA-dashboard
- Monitoringtools (bv. Zabbix, Nagios)
- Rapportagesystemen

SURF-relevantie:

Ondersteunt norm SC.01: beschikbaarheid, onderhoud en ondersteuning moeten meetbaar zijn. KPI's kunnen ook betrekking hebben op beveiligingsmaatregelen (bv. patch-tijd).

.

4. Prioritering en escalatie

- Incidentclassificatie (P1 t/m P4).
- Escalatieprocedures bij overschrijding van serviceniveaus

Waarom van belang:

Zorgt voor snelle en passende reactie op incidenten. Voorkomt dat kritieke issues blijven liggen.

Instrumenten:

- Incidentclassificatiematrix
- Escalatieprotocol
- ITSM-platforms (bv. TOPdesk, Jira Servicedesk, ServiceNow)

SURF-relevantie:

Essentieel voor incidentrespons en meldplicht bij datalekken. Escalatieprocedures moeten afgestemd zijn op beveiligingsimpact.

5. Monitoring en rapportage

- Frequentie en vorm van rapportages.
- Tools en methoden voor meting.

Waarom van belang:

Maakt prestaties transparant en biedt input voor verbeteringen. Ondersteunt governance en compliance.

Instrumenten:

- Periodieke SLA-rapportages
- Real-time dashboards
- SLA-reviewmeetings

SURF-relevantie:

Verplicht voor toetsing van beveiligingsmaatregelen. Rapportages kunnen input zijn voor audits en ketentoetsing.

6. Boetes en beloningen

- Service credits bij niet-naleving.
- Bonussen bij overprestatie

Waarom van belang:

Creëert prikkels voor naleving. Zorgt voor compensatie bij onderprestatie.

Instrumenten:

- Service credits
- Bonusmechanismen
- Contractuele boetebepalingen (vaak niet in SLA maar in contract)

SURF-relevantie:

Ondersteunt risicobeheersing. Bij uitbesteding aan derden is het belangrijk dat sancties ook gelden voor subverwerkers.

7. Wijzigingsbeheer

- Procedure voor het aanpassen van SLA-afspraken.
- Periodieke reviewmomenten

Waarom van belang:

Maakt SLA's flexibel en toekomstbestendig. Voorkomt dat afspraken verouderen.

Instrumenten:

- Change management proces
- SLA-reviewkalender
- Governanceboard

SURF-relevantie:

Beveiligingsmaatregelen en wetgeving (zoals AVG) veranderen regelmatig. SLA's moeten hierop kunnen anticiperen.

8. Feedbackmechanismen

Input van eindgebruikers en stakeholders.

Gebruik van eXperience Level Agreements (XLA's) om klantbeleving te meten

Waarom van belang:

Verbetert klantgerichtheid en gebruikerservaring. Helpt bij het identificeren van knelpunten.

Instrumenten:

- XLA's (Experience Level Agreements)
- Klanttevredenheidsonderzoeken
- Gebruikerspanels

SURF-relevantie:

Ondersteunt continue verbetering van beveiligingsbewustzijn en dienstverlening binnen onderwijsinstellingen.

9. Beëindiging en exitstrategie

- Voorwaarden voor beëindiging van de SLA.
- Overdracht van diensten bij contractbeëindiging.

SURF Normenkader Niveau 3 – Specifieke SLA-eisen

Het SURF Normenkader niveau 3 stelt eisen aan SLA's in het kader van informatiebeveiliging en ketenbeheer. Belangrijke aandachtspunten:

1. Norm SC.01 – Service Level Agreement

SLA moet expliciet ingaan op:

- Onderhoudsafspraken van IT-componenten.
- Ondersteuning bij incidenten en wijzigingen.
- Beveiligingsmaatregelen en compliance met ISO 27001/2:2022

2. Beveiligingsverplichtingen

Afspraken over:

- Patchmanagement.
- Logging en monitoring.
- Incidentrespons (incl. meldplicht datalekken).
- Continuïteitsbeheer (bv. back-up en herstelprocedures).

3. Ketenbeheer

- Verantwoordelijkheden bij uitbesteding aan derden.
- Transparantie over subverwerkers.
- Afspraken over overdracht van data en systemen.

4. Audits en toetsing

- Recht op audits door afnemer of externe partij.
- Periodieke toetsing op naleving van beveiligingsnormen.

5. Privacy en AVG

- Verwerkersovereenkomst als onderdeel of bijlage.
- Duidelijke afspraken over dataminimalisatie, bewaartermijnen en datadoorgifte.

Waarom van belang:

Beschermt persoonsgegevens en voorkomt juridische risico's. Verplicht onder Europese wetgeving.

Instrumenten:

- Verwerkersovereenkomst
- DPIA's (Data Protection Impact Assessments)
- AVG-checklists

SURF-relevantie:

AVG is integraal onderdeel van SURF Normenkader. SLA moet expliciet ingaan op dataminimalisatie, bewaartermijnen en datadoorgifte.