

Service Level Agreement

<opdrachtgever>

 **Safeguard**

Inhoudsopgave

Inleiding	3
Diensten	4
Veiligheid & Beveiliging	5
Beveiliging	5
Back-up	5
IT-Service Continuity Management	6
Service Levels	7
Governance rondom de communicatie en escalatie.	9
Exit strategie	10

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 2 van 10

Inleiding

Deze Service Level Agreement bevat de services aangeboden door Safeguard aan Opdrachtgever, evenals alle gerelateerde services die worden geleverd door Safeguard, zoals bepaald door de overeengekomen specificaties en service niveaus.

Deze SLA bepaalt meer specifiek:

1. wijze waarop de Opdrachtgever wordt geïnformeerd over uitgevoerde beveiligingstesten en de bevindingen daaruit;
2. IT-Service Continuity management;
3. service levels en uitbreiding daarop die aangeboden wordt maar niet gevraagd is door Opdrachtgever;
4. openstelling en Beschikbaarheid (ook van Helpdesk);
5. SLA Rapportages;
6. governance rondom de communicatie en escalatie.

Herzieningen van deze SLA zullen, indien nodig, de services en alle gerelateerde functionele, technische en organisatorische vragen bespreken die van toepassing zijn op grond van deze SLA. Mocht een dergelijke discussie leiden tot een Revisie van de diensten die door Safeguard aan Opdrachtgever worden geleverd, wordt de Revisie pas van kracht nadat alle partijen hun schriftelijke toestemming hebben gegeven.

Verband met andere documenten:

Deze SLA is een bijlage bij de Algemene voorwaarden. Alle artikelen in de overeenkomst zijn van toepassing op deze SLA.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 3 van 10

Diensten

De diensten die Safeguard aan Opdrachtgever levert, bestaan uit de volgende componenten:

- beheren infrastructuur (hosting);
- technisch beheer;
- technisch applicatiebeheer.

Deze componenten zijn onlosmakelijk met elkaar verbonden en zorgen ervoor dat de applicaties van de Opdrachtgever beschikbaar zijn voor de geautoriseerde gebruikers van de deelnemers.

Safeguard voert de volgende activiteiten uit:

- Installeren en beheren van een technische serverinfrastructuur waarmee alle toepassingen van de Opdrachtgever kunnen worden geïnstalleerd. Inbegrepen in de technische infrastructuur zijn: datacenters, servers, opslagvoorzieningen, back-up- en herstel voorzieningen en alle administratieve software die nodig is om de applicaties beschikbaar te maken, inclusief eventuele patches / updates en mogelijke foutoplossingen;
- Het zekerstellen van de overeengekomen beschikbaarheid van de service te behouden gedurende de in de Raamovereenkomst verleende periode met behulp van de daarvoor noodzakelijke middelen, methoden en technieken gebruikt;
- Het monitoren van alle systemen 24 uur per dag, zeven dagen per week;
- Het beschikbaar stellen van logboek faciliteiten voor het genereren van SLA rapportages en trendanalyses.
- Inrichten van een Servicedesk waar alle meldingen door Opdrachtgever 24/7 telefonisch, per e-mail en via Safeguard support kunnen worden ingediend;
- De afhandeling van incidenten en problemen -binnen de macht van Safeguard - gemeld door Opdracht aan de Support Desk, of waargenomen door Safeguard;
- De juiste toepassing van bronnen, methoden en technieken om de veiligheid, betrouwbaarheid en integriteit van de gegevens en bedrijfsomgeving van Opdrachtgever te waarborgen.
- De juiste toepassing van bronnen, methoden en technieken om verlies van gegevens van Opdrachtgever te voorkomen. Alle gegevens en geïnstalleerde software producten, inclusief configuratie-instellingen, worden periodiek beveiligd via back-up- en herstelprocedures;
- Het leveren van periodieke updates via e-mail aan Opdrachtgever, om deze op de hoogte te stellen over uitgevoerde beveiligingstesten en de bevindingen daaruit;

De serviceniveaus kunnen niet worden gerealiseerd in het geval van:

- onjuist gebruik door gebruikers Opdrachtgevers;
- incidenten en problemen veroorzaakt door softwarefouten, bijvoorbeeld Bugs in besturingssystemen van iOS of Android.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 4 van 10

Veiligheid & Beveiliging

Opdrachtnemer hanteert een beleid waarin beveiligingsmaatregelen gedetailleerd zijn beschreven en waarin de werking van de maatregelen op regelmatige basis wordt geverifieerd. Opdrachtnemer draagt zorg voor adequate beveiliging van de toegang tot Safeguard. Hieronder wordt onder meer verstaan:

- hardening van servers;
- scheiding van productie en acceptatie omgeving;
- versleuteling van gevoelige gegevens bij transport (SSL);
- het periodiek (minimaal jaarlijks) uitvoeren van kwetsbaarheden scans en penetratietesten.

Na beëindiging van de Overeenkomst draagt Opdrachtnemer zorg voor de overdracht van alle data op de wijze zoals omschreven onder Exit Strategie.

Beveiliging

De omgeving waarin de dienst draait wordt jaarlijks geaudit door een onafhankelijke auditor. Hierbij worden ook periodiek een kwetsbaarheden onderzoek en een penetratietest uitgevoerd. Opdrachtnemer is bereid mee te werken aan beveiligingsaudits, certificeringen door externe partijen. Het is Opdrachtgever zonder uitdrukkelijke schriftelijke toestemming van Opdrachtnemer niet toegestaan poortscans of kwetsbaarheden scans uit te voeren c.q. uit te laten voeren op safeguardapp.nl en subdomeinen die daaronder vallen. Indien noodzakelijk zal Opdrachtnemer in alle redelijkheid hieraan medewerking verlenen. Opdrachtgever wordt jaarlijks geïnformeerd over de bevindingen en opvolgacties die voortkomen uit het rapport van de auditor. De Opdrachtgever zal een contactpersoon voor informatiebeveiliging aanwijzen die voor de Opdrachtnemer het aanspreekpunt is indien er zich een beveiligingsincident voordoet.

Back-up

Dagelijks wordt er een Back-up gemaakt van de data. De systemen staan opgesteld in beveiligde datacenters die aan de hoogste kwaliteitseisen voldoen en ISO 27001 gecertificeerd zijn. Uitsluitend geautoriseerd personeel heeft toegang tot deze omgeving.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 5 van 10

IT-Service Continuity Management

Voor snel herstel bij calamiteiten heeft Safeguard een beslissingsstructuur en organisatie ingericht (zie Tabel 1). In geval van een ernstige calamiteit is er een Herstelplan en een Uitwijkplan in plaats. Onze hosting partner AWS past een eigen Business Continuity Management proces toe met daaropvolgend een IT Service Continuity Management proces. In Tabel 1 wordt dit beknopt weergegeven.

Tabel 1: Beslissingsstructuur

Rol	Normaal	Crisis
Directie	- BCM-beleid en -strategie vaststellen - Mensen en middelen regelen - Proces bevoegdheden regelen	- Crisis management - Corporate/Business - Externe Contacten
Management	- Process Management - Acceptatie van BCM-producten - Communicatie en bewustwording - Integratie ITSCM binnen BCM - Uitvoeren risico analyse - Producten definiëren - Contracten opstellen - Testen uitvoeren	- Coördinatie - Processturing - Beschikbaar stellen van middelen - Starten van continuity en recovery - Teamleiding - Rapportage
Personeel	- Producten ontwikkelen - Onderhandelen - Tests uitvoeren - Rapporten maken - Procedures ontwikkelen	- Uitvoeren recovery - Teamwerk

Als zich een calamiteit heeft voorgedaan wordt er gerapporteerd over de oorzaak en de gevolgen. Tekortkomingen in de plannen leiden tot wijzigingsvoorstellen in de contingency plannen. Van alle tests worden rapportages aan het management verstrekt. Ook over nieuwe risico's wordt regelmatig aan het management gerapporteerd.

Service Levels

Servicedesk uren

Maandag tot en met vrijdag van 07.00 tot 18.00 uur, met uitzondering van officiële feestdagen.

Kantoortijden

Maandag tot en met vrijdag van 07.00 tot 18.00 uur, met uitzondering van officiële feestdagen.

Servicedesk beschikbaarheid

Telefoon: +31 (0) 859021090

E-mail: support@safeguardapp.nl

Incidenten en suggesties kunnen 24/7 per e-mail worden gemeld.

Incidenten met een hoge prioriteit kunnen 24/7 worden gemeld via het vermelde telefoonnummer. Incidenten met hoge prioriteit moeten telefonisch worden gemeld. De afhandeling van dergelijke incidenten gebeurt 24/7. Alle andere oproepen worden afgehandeld tijdens de reguliere servicedesk-uren.

Reactietijden Servicedesk:

- Incidenten met de hoogste prioriteit hebben, tijdens Servicedesk uren, een reactietijd van vijftien minuten. Na service desk uren is de reactietijd één uur.
- Incidenten met een normale prioriteit hebben, tijdens Servicedesk uren, een reactietijd van vier uur. Na service desk uren is de reactietijd 24 uur.

Oplostijden:

- Incidenten met de hoogste prioriteit hebben een oplostijd van maximaal vier uur.
- Incidenten met een normale prioriteit hebben geen specifieke oplostijd; deze oplostijd is nader te bepalen.

Indien een bug in de app aanleiding is voor een storing, moet er een nieuwe release van de app worden uitgebracht om de storing op te kunnen lossen. Nieuwe versies van de apps met oplossingen moeten goedgekeurd worden door Apple en Google, hier heeft Opdrachtnemer geen invloed op en kan dus een onbepaalde tijd duren. Safeguard beoordeelt in overleg met Opdrachtgever de prioriteit van het probleem. De responstijden voor incidenten met een hoge prioriteit zijn alleen van toepassing als ze telefonisch worden ingediend en zijn niet van toepassing op incidenten die zijn ingediend via de ondersteuningssite of via e-mail.

Beschikbaarheid Safeguard-app:

- De beschikbaarheid Safeguard app tijdens Werkdagen tussen 07.00 uur en 21.00 uur bedraagt minimaal 99,60%.
- De beschikbaarheid buiten de hierboven genoemde tijden bedraagt minimaal 96,10%;
- De MTBF is minimaal 100 dagen.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 7 van 10

- De MTTR voor onderbrekingen langer dan drie minuten bedraagt maximaal vier uur.
- Het aantal onderbrekingen van drie minuten of korter treden maximaal tweemaal per maand op.
- Managementrapportages worden binnen drie weken na afloop van elk kalenderkwartaal opgeleverd.

Monitoring (additioneel):

24/7 actieve monitoring met volledige ondersteuning voor incidenten binnen en buiten kantooruren.

Rapportages

Managementrapportages (zie Tabel 2) worden binnen drie weken na afloop van elk kalenderkwartaal opgeleverd. In deze rapportages worden per rapportage niveau de gegevens kenbaar gemaakt.

Tabel 2: Rapportage overzicht

Functioneel beheerder rapportages	Locatie beheerder (deelnemer) rapportages
Afwijkingen op de beveiligingsaspecten, capaciteit en Performance.	Actuele gebruikers en hun autorisatie
Inzicht in de Beschikbaarheid van de Safeguard-app bij de Deelnemer.	Afwijkingen op de beveiligingsaspecten, capaciteit en Performance.
Safeguard levert per Deelnemer een overzicht op van de aangesloten locaties van die Deelnemer.	Inzicht in de Beschikbaarheid van de Safeguard-app bij de Deelnemer.
Safeguard levert eenmaal per jaar aan Opdrachtgever een overzicht van de data waarop audits betreffende security / privacy / certificering / accountantsverklaring hebben plaatsgevonden en de wijze waarop verbeterpunten in de processen zijn verwerkt.	Safeguard levert per Deelnemer een overzicht op van de aangesloten locaties van die Deelnemer. Aanvullend dient gerapporteerd te worden over de nieuw aangesloten en/of beëindigde aansluitingen op de Safeguard-app onder vermelding van de NAWgegevens van de locatie inclusief aansluiten/of beëindigingsdatum.

Governance rondom de communicatie en escalatie.

Escalaties met betrekking tot incidenten en wijzigingen kunnen alleen plaatsvinden op het moment dat de servicelevels, zoals gedefinieerd, worden overtreden of waarschijnlijk zullen worden overtreden. De communicatie van de escalatie is gebaseerd op de escalatiematrix (zie Tabel 3).

Escalatieprocedure van Opdrachtgever dient in samenwerking met Opdrachtgever opgesteld te worden.

Tabel 3: Escalatiematrix

Naam	Functie	Contactgegevens	Beschikbaarheid
Operationeel	Service Desk	Telefoon: 0859021090 Email: support@safeguardapp.nl	24/7
Escalatie 1	Implementatie manager	Telefoon: 0859021090 Email: implementatie@safeguardapp.nl	24/7
Escalatie 2	Kwaliteitsmanager	Telefoon: 0859021090 Email: kwaliteit@safeguardapp.nl	24/7
Escalatie 3	Directie	Telefoon: +31651530420 Email: directie@safeguardapp.nl	24/7

Exit strategie

Bij het beëindigen van de overeenkomst treedt de exitstrategie van Safeguard in werking. Deze wordt jaarlijks getoetst aan de hand van ISO 9001, ISO 27001 en ISO 27701 met de betreffende certificering als gevolg. We hanteren hiervoor de volgende opzet:

1. Bij beëindiging van de gebruiksovereenkomst vervalt de mogelijkheid om gebruik te maken van de Safeguard app.
2. De voorwaarden met betrekking tot het gebruik van de Safeguard app zijn vastgelegd in de overeenkomst die met Opdrachtgever gesloten is.
3. Het exitplan dat Safeguard hanteert is van toepassing zowel bij de afloop van de overeenkomst als in die gevallen waarbij mogelijk de overeenkomst niet afgelopen is maar wel de relatie met Safeguard als opdrachtnemer stopt, om welke reden dan ook.
4. De werking van de eventueel gesloten verwerkersovereenkomst is van toepassing tot en met het moment dat de uitvoering van het exitplan is afgerond. In de praktijk zal dit betekenen dat de overdracht van de data heeft plaatsgevonden.
5. Bij de verstrekking van de data, op basis van het exitplan, zal Safeguard een overzicht toevoegen aan de hand waarvan gecontroleerd kan worden of de overdracht van de data compleet is. In afstemming met Opdrachtgever zal Safeguard bij aanvang van onze relatie door middel van de door Opdrachtgever beschikbare gestelde verwerkersovereenkomst vastleggen welke data door Safeguard wordt verwerkt en opgeslagen en op welke wijze de compleetheid van deze data kan worden gecontroleerd in geval van exit.
6. De data die met behulp van de app worden verwerkt en gegenereerd kan Safeguard desgewenst aan Opdrachtgever ter beschikking stellen. Safeguard hanteert als standaard formaat JSON. Het formaat van de op te leveren data wordt op het moment van een exit in overleg vastgesteld. Safeguard zal de data ter beschikking stellen vanaf 90 dagen voor de datum van afloop van het gebruiksrecht.
7. Opdrachtgever ontvangt bij een eventuele terbeschikkingstelling alle beschikbare data.
8. In het bestand dat Safeguard op basis van het exit plan aan Opdrachtgever zal verstrekken is een beknopte beschrijving toegevoegd waarmee de betekenis van de verschillende data (elementen) duidelijk wordt. Deze informatie kan eventueel worden gebruikt bij het verwerken van de data bij een nieuwe applicatie.
9. Het exitplan zal maximaal 30 dagen na beëindiging van de gebruiksovereenkomst volbracht zijn tenzij in onderling overleg anders wordt besloten.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 10 van 10