

# Service Level Agreement

<Auftraggeber>

 **Safeguard**

# Inhoudsopgave

|                                                      |           |
|------------------------------------------------------|-----------|
| Einleitung                                           | 3         |
| Dienstleistungen                                     | 4         |
| Sicherheit & Schutz                                  | 6         |
| Sicherheit                                           | 6         |
| Backup                                               | 6         |
| IT-Service Continuity Management                     | 7         |
| Service Levels                                       | 8         |
| Governance in Bezug auf Kommunikation und Eskalation | 11        |
| Exit-Strategie                                       | <b>12</b> |

| Klassifikation | Copyright ©    | Seite          |
|----------------|----------------|----------------|
| Vertraulich    | Safeguard B.V. | Seite 2 von 12 |

# Einleitung

Diese Service Level Agreement enthält die von Safeguard angebotenen Dienstleistungen für den Auftraggeber sowie alle damit verbundenen Dienstleistungen, die von Safeguard gemäß den vereinbarten Spezifikationen und Serviceniveaus erbracht werden.

Diese SLA legt insbesondere Folgendes fest:

1. die Art und Weise, wie der Auftraggeber über durchgeführte Sicherheitstests und die daraus resultierenden Erkenntnisse informiert wird;
2. das IT-Service-Continuity-Management;
3. Serviceniveaus und Erweiterungen, die angeboten, aber vom Auftraggeber nicht angefordert wurden;
4. Öffnungszeiten und Verfügbarkeit (auch des Helpdesks);
5. SLA-Berichte;
6. Governance im Hinblick auf Kommunikation und Eskalation.

Überarbeitungen dieser SLA werden – sofern erforderlich – die Dienstleistungen sowie alle damit verbundenen funktionalen, technischen und organisatorischen Fragestellungen behandeln, die im Rahmen dieser SLA relevant sind. Sollte eine solche Diskussion zu einer Überarbeitung der von Safeguard für den Auftraggeber erbrachten Dienstleistungen führen, tritt die Überarbeitung erst in Kraft, nachdem alle Parteien ihre schriftliche Zustimmung erteilt haben.

Verbindung zu anderen Dokumenten:

Diese SLA ist eine Anlage zu den Allgemeinen Geschäftsbedingungen. Alle Bestimmungen der Vereinbarung gelten auch für diese SLA.

| Klassifikation | Copyright ©    | Seite          |
|----------------|----------------|----------------|
| Vertraulich    | Safeguard B.V. | Seite 3 von 12 |

# Dienstleistungen

Die von Safeguard für den Auftraggeber erbrachten Dienstleistungen bestehen aus den folgenden Komponenten:

- Verwaltung der Infrastruktur (Hosting);
- Technisches Management;
- Technische Anwendungsverwaltung.

Diese Komponenten sind untrennbar miteinander verbunden und gewährleisten die Verfügbarkeit der Anwendungen des Auftraggebers für die autorisierten Nutzer der teilnehmenden Parteien.

Safeguard führt die folgenden Aktivitäten durch:

- Installation und Verwaltung einer technischen Serverinfrastruktur, auf der alle Anwendungen des Auftraggebers installiert werden können. Zur technischen Infrastruktur gehören: Rechenzentren, Server, Speichereinrichtungen, Backup- und Wiederherstellungseinrichtungen sowie alle administrativen Softwarekomponenten, die zur Bereitstellung der Anwendungen erforderlich sind, einschließlich etwaiger Patches/Updates und möglicher Fehlerbehebungen;
- Sicherstellung der vereinbarten Verfügbarkeit der Services während der in der Rahmenvereinbarung festgelegten Laufzeit unter Einsatz der dafür notwendigen Ressourcen, Methoden und Techniken;
- Überwachung aller Systeme rund um die Uhr, sieben Tage die Woche;
- Bereitstellung von Protokollierungsfunktionen zur Erstellung von SLA-Berichten und Trendanalysen;
- Einrichtung eines Service-Desks, bei dem der Auftraggeber rund um die Uhr telefonisch, per E-Mail und über den Safeguard-Support Meldungen einreichen kann;
- Bearbeitung von Vorfällen und Problemen – soweit im Einflussbereich von Safeguard – die vom Auftraggeber an den Support Desk gemeldet oder von Safeguard selbst festgestellt werden;
- Anwendung geeigneter Ressourcen, Methoden und Techniken zur Gewährleistung der Sicherheit, Zuverlässigkeit und Integrität der Daten und der Betriebsumgebung des Auftraggebers;
- Anwendung geeigneter Ressourcen, Methoden und Techniken zur Vermeidung von Datenverlust des Auftraggebers. Alle Daten und installierten Softwareprodukte, einschließlich der Konfigurationseinstellungen, werden regelmäßig durch Backup- und Wiederherstellungsverfahren gesichert;
- Bereitstellung regelmäßiger Updates per E-Mail an den Auftraggeber zur Information über durchgeführte Sicherheitstests und die daraus gewonnenen Erkenntnisse.

| Klassifikation | Copyright ©    | Seite          |
|----------------|----------------|----------------|
| Vertraulich    | Safeguard B.V. | Seite 4 von 12 |

Die Serviceniveaus können in folgenden Fällen nicht gewährleistet werden:

- unsachgemäße Nutzung durch die Benutzer des Auftraggebers;
- Vorfälle und Probleme, die durch Softwarefehler verursacht werden, beispielsweise Bugs in Betriebssystemen wie iOS oder Android.

| Klassifikation | Copyright ©    | Seite          |
|----------------|----------------|----------------|
| Vertraulich    | Safeguard B.V. | Seite 5 von 12 |

# Sicherheit & Schutz

Der Auftragnehmer verfolgt eine Richtlinie, in der Sicherheitsmaßnahmen detailliert beschrieben sind und deren Wirksamkeit regelmäßig überprüft wird.

Der Auftragnehmer gewährleistet eine angemessene Absicherung des Zugangs zu Safeguard. Dazu gehören unter anderem:

- Härtung der Server;
- Trennung von Produktions- und Abnahmeumgebungen;
- Verschlüsselung sensibler Daten während der Übertragung (SSL);
- regelmäßige Durchführung (mindestens jährlich) von Schwachstellenanalysen und Penetrationstests.

Nach Beendigung des Vertrags stellt der Auftragnehmer die Übergabe sämtlicher Daten in der unter „Exit-Strategie“ beschriebenen Weise sicher.

## Sicherheit

Die Umgebung, in der der Dienst betrieben wird, wird jährlich von einem unabhängigen Auditor geprüft. Dabei werden auch regelmäßig Schwachstellenanalysen und Penetrationstests durchgeführt. Der Auftragnehmer ist bereit, an Sicherheitsprüfungen und Zertifizierungen durch externe Parteien mitzuwirken. Dem Auftraggeber ist es ohne ausdrückliche schriftliche Zustimmung des Auftragnehmers nicht gestattet, Port-Scans oder Schwachstellenanalysen auf Safeguardapp.nl und den dazugehörigen Subdomains durchzuführen oder durchführen zu lassen. Falls erforderlich, wird der Auftragnehmer in angemessenem Umfang seine Mitwirkung gewähren. Der Auftraggeber wird jährlich über die Ergebnisse und Folgemaßnahmen aus dem Bericht des Auditors informiert. Der Auftraggeber benennt eine Kontaktperson für Informationssicherheit, die im Falle eines Sicherheitsvorfalls als Ansprechpartner für den Auftragnehmer fungiert.

## Backup

Täglich wird eine Sicherung (Backup) der Daten erstellt. Die Systeme befinden sich in gesicherten Rechenzentren, die den höchsten Qualitätsanforderungen entsprechen und nach ISO 27001 zertifiziert sind. Der Zugang zu dieser Umgebung ist ausschließlich autorisiertem Personal gestattet.

| Klassifikation | Copyright ©    | Seite          |
|----------------|----------------|----------------|
| Vertraulich    | Safeguard B.V. | Seite 6 von 12 |

# IT-Service Continuity Management

Für eine schnelle Wiederherstellung im Falle von Notfällen hat Safeguard eine Entscheidungsstruktur und Organisation eingerichtet (siehe Tabelle 1). Im Falle eines schwerwiegenden Notfalls stehen ein Wiederherstellungsplan sowie ein Ausweichplan zur Verfügung. Unser Hosting-Partner AWS wendet ein eigenes Business-Continuity-Management-Verfahren an, dem ein IT-Service-Continuity-Management-Prozess folgt. Eine kompakte Darstellung ist in Tabelle 1 zu finden.

Tabelle 1: Entscheidungsstruktur

| Rolle            | Normalbetrieb                                                                                                                                                                                                                                                                                                                                  | Krisenfall                                                                                                                                                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Geschäftsführung | <ul style="list-style-type: none"><li>- Festlegung der BCM-Richtlinien und -Strategie</li><li>- Bereitstellung von Personal und Ressourcen</li><li>- Regelung der Prozessbefugnisse</li></ul>                                                                                                                                                  | <ul style="list-style-type: none"><li>- Krisenmanagement</li><li>- Corporate/Business</li><li>- Externe Kontakte</li></ul>                                                                                                                      |
| Management       | <ul style="list-style-type: none"><li>- Prozessmanagement</li><li>- Abnahme der BCM-Produkte</li><li>- Kommunikation und Sensibilisierung</li><li>- Integration des ITSCM in das BCM</li><li>- Durchführung von Risikoanalysen</li><li>- Definition der Produkte</li><li>- Erstellung von Verträgen</li><li>- Durchführung von Tests</li></ul> | <ul style="list-style-type: none"><li>- Koordination</li><li>- Prozesssteuerung</li><li>- Bereitstellung von Ressourcen</li><li>- Einleitung von Continuity- und Recovery-Maßnahmen</li><li>- Teamleitung</li><li>- Berichterstattung</li></ul> |
| Personal         | <ul style="list-style-type: none"><li>- Entwicklung von Produkten</li><li>- Verhandlungen führen</li><li>- Durchführung von Tests</li><li>- Erstellung von Berichten</li><li>- Entwicklung von Verfahren</li></ul>                                                                                                                             | <ul style="list-style-type: none"><li>- Durchführung der Wiederherstellung (Recovery)</li><li>- Teamarbeit</li></ul>                                                                                                                            |

Im Falle eines eingetretenen Notfalls wird über die Ursache und die Auswirkungen Bericht erstattet. Mängel in den Plänen führen zu Änderungsvorschlägen für die Notfallpläne (Contingency-Pläne). Über alle durchgeführten Tests werden dem Management Berichte vorgelegt. Auch über neue Risiken wird das Management regelmäßig informiert.

## Service Levels

### *Servicezeiten des Servicedesks*

Montag bis Freitag von 07:00 bis 18:00 Uhr, ausgenommen gesetzliche Feiertage.

### *Bürozeiten*

Montag bis Freitag von 07:00 bis 18:00 Uhr, ausgenommen gesetzliche Feiertage.

### *Verfügbarkeit des Servicedesks*

Telefon: +31 (0) 859021090

E-mail: [support@Safeguardapp.nl](mailto:support@Safeguardapp.nl)

Vorfälle und Vorschläge können rund um die Uhr per E-Mail gemeldet werden.

Vorfälle mit hoher Priorität können rund um die Uhr über die angegebene Telefonnummer gemeldet werden. Solche Vorfälle müssen telefonisch gemeldet werden. Die Bearbeitung dieser Vorfälle erfolgt ebenfalls 24/7. Alle anderen Anfragen werden während der regulären Servicezeiten des Servicedesks bearbeitet.

### *Reaktionszeiten des Servicedesks:*

- Vorfälle mit der höchsten Priorität haben während der Servicezeiten eine Reaktionszeit von 15 Minuten. Außerhalb der Servicezeiten beträgt die Reaktionszeit eine Stunde.
- Vorfälle mit normaler Priorität haben während der Servicezeiten eine Reaktionszeit von vier Stunden. Außerhalb der Servicezeiten beträgt die Reaktionszeit 24 Stunden.

### *Lösungszeiten:*

- Vorfälle mit der höchsten Priorität müssen innerhalb von maximal vier Stunden behoben sein.
- Vorfälle mit normaler Priorität haben keine festgelegte Lösungszeit; diese wird gesondert festgelegt.

Wenn ein Fehler in der App die Ursache für eine Störung ist, muss eine neue Version der App veröffentlicht werden, um die Störung zu beheben. Neue Versionen der Apps mit entsprechenden Lösungen müssen von Apple und Google genehmigt werden – auf diesen Prozess hat der Auftragnehmer keinen Einfluss, und die Dauer kann daher unbestimmt sein.

Safeguard bewertet in Absprache mit dem Auftraggeber die Priorität des Problems. Die Reaktionszeiten für Vorfälle mit hoher Priorität gelten ausschließlich bei telefonischer Meldung

| Klassifikation | Copyright ©    | Seite          |
|----------------|----------------|----------------|
| Vertraulich    | Safeguard B.V. | Seite 8 von 12 |

und finden keine Anwendung auf Vorfälle, die über die Support-Website oder per E-Mail gemeldet wurden.

*Verfügbarkeit der Safeguard-App:*

- Die Verfügbarkeit der Safeguard-App an Werktagen zwischen 07:00 Uhr und 21:00 Uhr beträgt mindestens 99,60 %.
- Die Verfügbarkeit außerhalb der oben genannten Zeiten beträgt mindestens 96,10 %.
- Die MTBF (Mean Time Between Failures) beträgt mindestens 100 Tage.
- Die MTTR (Mean Time To Repair) für Unterbrechungen, die länger als drei Minuten andauern, beträgt maximal vier Stunden.
- Die Anzahl der Unterbrechungen mit einer Dauer von drei Minuten oder kürzer ist auf höchstens zwei pro Monat begrenzt.
- Managementberichte werden innerhalb von drei Wochen nach Ablauf jedes Kalendervierteljahres bereitgestellt.

*Monitoring (zusätzlich):*

24/7 aktive Überwachung mit vollständiger Unterstützung bei Vorfällen während und außerhalb der Bürozeiten.

*Berichte*

Managementberichte (siehe Tabelle 2) werden innerhalb von drei Wochen nach Ablauf jedes Kalendervierteljahres bereitgestellt. In diesen Berichten werden die Daten entsprechend der jeweiligen Berichtsebene offengelegt.

| Klassifikation | Copyright ©    | Seite          |
|----------------|----------------|----------------|
| Vertraulich    | Safeguard B.V. | Seite 9 von 12 |

Tabelle 2: Berichtsübersicht

| Berichte für den Funktionalen Administrator                                                                                                                                                                                                                                                                  | Berichte für den Standortverwalter (Teilnehmer)                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Abweichungen in Bezug auf Sicherheitsaspekte, Kapazität und Performance.                                                                                                                                                                                                                                     | Aktuelle Benutzer und deren Berechtigungen                                                                                                                                                                                                                                                                                                                 |
| Einblick in die Verfügbarkeit der Safeguard-App beim Teilnehmer.                                                                                                                                                                                                                                             | Abweichungen in den Bereichen Sicherheit, Kapazität und Leistung.                                                                                                                                                                                                                                                                                          |
| Safeguard stellt für jeden Teilnehmer eine Übersicht der angeschlossenen Standorte dieses Teilnehmers zur Verfügung.                                                                                                                                                                                         | Einblick in die Verfügbarkeit der Safeguard-App beim jeweiligen Teilnehmer.                                                                                                                                                                                                                                                                                |
| Safeguard stellt dem Auftraggeber einmal jährlich eine Übersicht der Daten zur Verfügung, an denen Audits in Bezug auf Sicherheit / Datenschutz / Zertifizierungen / Wirtschaftsprüfererklärungen stattgefunden haben, sowie eine Darstellung, wie Verbesserungsmaßnahmen in die Prozesse integriert wurden. | Safeguard stellt für jeden Teilnehmer eine Übersicht der angeschlossenen Standorte dieses Teilnehmers zur Verfügung. Ergänzend wird über neu angeschlossene und/oder beendete Verbindungen zur Safeguard-App berichtet, einschließlich der Angabe der Adressdaten (Name, Anschrift, Wohnort) des Standorts sowie des Datums der Anbindung bzw. Beendigung. |

# Governance in Bezug auf Kommunikation und Eskalation

Eskalationen im Zusammenhang mit Vorfällen und Änderungen können nur dann erfolgen, wenn die definierten Servicelevels verletzt wurden oder voraussichtlich verletzt werden. Die Kommunikation im Rahmen der Eskalation erfolgt auf Grundlage der Eskalationsmatrix (siehe Tabelle 3).

Das Eskalationsverfahren des Auftraggebers ist in Zusammenarbeit mit dem Auftraggeber auszuarbeiten.

Tabelle 3: Eskalationsmatrix

| Name         | Funktion                | Kontaktdaten                                                | Verfügbarkeit |
|--------------|-------------------------|-------------------------------------------------------------|---------------|
| Operativ     | Service-Desk            | Telefon: 0859021090<br>Email: support@Safeguardapp.nl       | 24/7          |
| Escalation 1 | Implementierungsmanager | Telefon: 0859021090<br>Email: implementatie@Safeguardapp.nl | 24/7          |
| Escalation 2 | Qualitätsmanager        | Telefon: 0859021090<br>Email: kwaliteit@Safeguardapp.nl     | 24/7          |
| Escalation 3 | Geschäftsführung        | Telefon: +31651530420<br>Email: directie@Safeguardapp.nl    | 24/7          |

# Exit-Strategie

Beim Beenden des Vertrags tritt die Exit-Strategie von Safeguard in Kraft. Diese wird jährlich anhand der Normen ISO 9001, ISO 27001 und ISO 27701 überprüft, was zur entsprechenden Zertifizierung führt. Dabei wird folgendes Vorgehen angewendet:

1. Mit Beendigung der Nutzungsvereinbarung erlischt die Möglichkeit, die Safeguard-App zu verwenden.
2. Die Bedingungen für die Nutzung der Safeguard-App sind in der mit dem Auftraggeber geschlossenen Vereinbarung festgelegt.
3. Der von Safeguard angewandte Exit-Plan gilt sowohl bei Ablauf der Vereinbarung als auch in Fällen, in denen die vertragliche Beziehung zu Safeguard als Auftragnehmer – aus welchem Grund auch immer – endet, ohne dass die Vereinbarung formell beendet wurde.
4. Die Gültigkeit einer gegebenenfalls geschlossenen Auftragsverarbeitungsvereinbarung bleibt bis zum Abschluss der Durchführung des Exit-Plans bestehen. In der Praxis bedeutet dies, dass die Datenübertragung erfolgt ist.
5. Bei der Übergabe der Daten im Rahmen des Exit-Plans wird Safeguard eine Übersicht beifügen, anhand derer überprüft werden kann, ob die Datenübertragung vollständig ist. In Abstimmung mit dem Auftraggeber wird Safeguard zu Beginn der Zusammenarbeit auf Grundlage der vom Auftraggeber zur Verfügung gestellten Auftragsverarbeitungsvereinbarung festlegen, welche Daten von Safeguard verarbeitet und gespeichert werden und wie im Falle eines Exits die Vollständigkeit dieser Daten überprüft werden kann.
6. Die durch die App verarbeiteten und generierten Daten kann Safeguard dem Auftraggeber auf Wunsch zur Verfügung stellen. Safeguard verwendet als Standardformat JSON. Das genaue Datenformat wird im Falle eines Exits in gegenseitigem Einvernehmen festgelegt. Safeguard stellt die Daten ab 90 Tagen vor Ablauf des Nutzungsrechts zur Verfügung.
7. Der Auftraggeber erhält bei einer etwaigen Bereitstellung sämtliche verfügbaren Daten.
8. Die von Safeguard im Rahmen des Exit-Plans bereitgestellte Datei enthält eine kurze Beschreibung, die die Bedeutung der verschiedenen Datenelemente erläutert. Diese Informationen können bei der Weiterverarbeitung der Daten in einer neuen Anwendung verwendet werden.
9. Der Exit-Plan wird spätestens 30 Tage nach Beendigung der Nutzungsvereinbarung abgeschlossen, sofern nicht in gegenseitigem Einvernehmen etwas anderes vereinbart wurde.

| Klassifikation | Copyright ©    | Seite           |
|----------------|----------------|-----------------|
| Vertraulich    | Safeguard B.V. | Seite 12 von 12 |