

Informationssicherheits- und Datenschutzplan

Informationssicherheit und Datenschutz bei Safeguard



Abteilung	Datenschutz
Firmenname	Safeguard B.V.
Contact	info@Safeguardapp.nl

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 1 von 36

Inhaltsverzeichnis

1. Einführung	4
1.1 Zweck	4
1.2 Leseführung	4
2. Physische Sicherheit und Sicherheit von Arbeitsumgebungen	5
2.1 Physischer Zugang zu Bürogebäuden	5
2.2 Physische Sicherheit von Rechenzentren	5
2.3 Physisches Gerätemanagement	6
2.3.1 Sicherheit von Computern und mobilen Geräten	6
2.3.2 Konfigurationsmanagement und Verteilung	6
3. Passwortrichtlinie und Kontozugriff	7
3.1 Passwortrichtlinie	7
3.2 Multi-Faktor-Authentifizierung (MFA)	8
3.3 Kontozugriff	8
4. Sicherheit IT	10
4.1 DDoS-Schutz	10
4.2 Kryptografie	10
4.3 Übertragung personenbezogener Daten	10
4.4 Penetrationstests (Pen-Testing)	10
4.5 Datenvalidierung	10
4.6 Malware, Härtung und Patchen	11
4.7 Sicherheitsprüfungen	11
5. Sicherheitsvorfälle	12
5.1 Vorfallmeldung	12
5.2 Vorfallbearbeitung	12
6. Software-Updates und Entwicklung	14
6.1 Entwicklungsprozess	14
6.2 Abhängigkeiten von Drittanbietern, Patches und Schwachstellen	15
6.3 Veröffentlichungspolitik	16
6.4 Quellcode und technische Dokumentation	17
6.5 Risikobewertung	17
7. Protokollierung	18
7.1 Rollenverteilung und Verantwortlichkeit	18
7.2 Protokollverwaltung	18
7.2.1 Protokolldateistruktur	18
7.2.2 Zu protokollierende Ereignisse	19
7.2.3 Ereignisse außerhalb des Protokollbereichs	20
7.2.4 Schutz der Protokolldateien	20
7.2.5 Zeitsynchronisation	20

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 2 von 36

7.3 Berichterstattung und Überwachung	21
7.3.1 Berichterstattung	21
7.3.2 Überwachung	21
7.3.3 Verteilung	21
8. Backup und Wiederherstellung	22
9. Verarbeitung personenbezogener Daten	23
9.1 Klassifizierung von Benutzerdaten	23
9.2 Ausstiegsstrategie	25
9.3 Unterauftragnehmer	25
10. Business Continuity Management (BCM)	26
10.1 IT-Service-Kontinuitätsmanagement	26
10.2 Treuhandvertrag	27
11. Personal	28
11.1 Überprüfung	28
11.2 Schulung	28
11.3 Vertraulichkeit	28
12. Sicherheitsrichtlinie	30
12.1 Von Vision, Mission bis Strategie	30
12.1.1 Dienstleistungen	30
12.1.2 Mission und Vision	30
12.1.3 Kernwerte	30
12.2 Vom Strategie zur Richtlinie	31
12.2.1 Ort der Information und Datenschutz	31
12.2.2 Konkrete Richtlinienpunkte	32

1. Einführung

Dieser Informationssicherheitsplan ist eine Ausarbeitung der Informationssicherheitspolitik.

1.1 Zweck

Der Zweck dieses Dokuments ist es, Einblicke in die derzeitigen Maßnahmen, Verfahren und Prozesse zu geben, die bei Safeguard implementiert wurden, um die Qualität der Informationssicherheit zu gewährleisten.

1.2 Leseführung

Kapitel 2 erklärt die Verfahren zum Schutz des physischen Zugangs zum Büro und zu den Servern.

Kapitel 3 erläutert die Verfahren rund um Passwortschutz, Multi-Faktor-Authentifizierung und die Autorisierungsmatrix.

Kapitel 4 erklärt, wie Safeguard mit Sicherheit in den Bereichen DDoS-Schutz, Kryptografie, Penetrationstests, Malware und Systemhärtung umgeht.

Kapitel 5 erläutert, wie der Prozess rund um das Melden von Sicherheitsvorfällen funktioniert.

Kapitel 6 beschreibt den Entwicklungsprozess bei Safeguard, wie Safeguard mit Patches umgeht, wie die Release-Politik strukturiert ist, wie die Dokumentationsprozesse ablaufen und wie das Risikomanagement sichergestellt wird.

Kapitel 7 erläutert, wie Safeguard mit Protokollierung, Rollenteilung und Verantwortlichkeit, Protokollverwaltung sowie Berichterstattung und Überwachung umgeht.

Kapitel 8 beschreibt die Backup- und Wiederherstellungsverfahren.

Kapitel 9 erklärt, welche persönlichen Daten Safeguard speichert und wie lange diese aufbewahrt werden, die Ausstiegsstrategie sowie eine Liste der Unterauftragsverarbeiter.

Kapitel 10 beschreibt, wie Safeguard mit dem Business Continuity Management umgeht.

Kapitel 11 beschreibt die Personalpolitik.

Kapitel 12 beschreibt die Sicherheitspolitik.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 4 von 36

2. Physische Sicherheit und Sicherheit von Arbeitsumgebungen

In diesem Kapitel wird erläutert, wie das Zugangsmanagement zu den Bürogebäuden, Geräten und zum Zugriff auf die Server bei Safeguard geregelt ist.

2.1 Physischer Zugang zu Bürogebäuden

Bei Beginn der Anstellung bei Safeguard erhalten alle Mitarbeiter Schlüssel, die Zugang zu unserem Bürogebäude ermöglichen. Die ausgegebenen Schlüssel werden in einem Überblick registriert. Für den vollständigen Zugang zum Büro sind mehrere Schlüssel erforderlich: Es gibt einen Schlüssel für den Rollladen vor der Tür, einen für die Haupteingangstür des Gebäudes und einen weiteren für das Büro selbst.

Das Büro ist mit einem Sicherheitsschlüssel gesichert, der ebenfalls bei Arbeitsbeginn bei Safeguard bereitgestellt wird. Der oder die Mitarbeiter, die als letzte das Gebäude verlassen, müssen alle Türen und Fenster im Büro schließen und den Alarm mit diesem Sicherheitsschlüssel wieder aktivieren.

Bevor der Rollladen an der Haupteingangstür des Gebäudes geschlossen wird, müssen die Mitarbeiter überprüfen, ob alle anderen Personen das Gebäude verlassen haben.

Zweimal im Jahr führt unser Gebäudemanager eine Überprüfung durch, um sicherzustellen, dass alle Schlüssel vorhanden und funktionsfähig sind. Alle Mitarbeiter sind verpflichtet, fehlende Schlüssel der Büroleitung zu melden.

Wenn nach der jährlichen Überprüfung ein oder mehrere Schlüssel fehlen oder die Anzahl der Schlüssel nicht korrekt ist, wird das folgende Verfahren angewandt:

1. Überprüfen, welche Person ein oder mehrere Schlüssel vermisst und welche spezifischen Schlüssel fehlen.
2. Überprüfen, wie lange die Schlüssel bereits fehlen.
3. Wenn Schlüssel am selben Tag verloren gehen, wird zunächst eine allgemeine Suche durchgeführt.
4. Wenn die Schlüssel bis 15:00 Uhr desselben Tages nicht gefunden werden, wird der Gebäudemanager informiert.

2.2 Physische Sicherheit von Rechenzentren

Safeguard nutzt ISO 27001- und FISMA-zertifizierte Rechenzentren, die von Amazon Web Services (AWS) verwaltet werden. AWS verfügt über langjährige Erfahrung in der Planung, dem

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 5 von 36

Bau und dem Betrieb von Rechenzentren im großen Maßstab. Weitere Informationen darüber, wie AWS seine Rechenzentren sichert, finden Sie auf deren Website.

2.3 Physisches Gerätemanagement

2.3.1 Sicherheit von Computern und mobilen Geräten

Computer und mobile Geräte dürfen nicht unverschlossen gelassen werden. Die automatische Sperrfunktion sollte aktiviert sein und sich nach maximal 5 Minuten einschalten. Wenn das Gerät verlassen wird, sollte es manuell gesperrt werden. Das Entsperren sollte mit einem Passwort erfolgen, das der Passwortrichtlinie entspricht, oder über biometrischen Zugang.

Mobile Geräte sollten, wenn möglich, Festplatten- und Datenverschlüsselung verwenden und möglichst keine Unternehmensinformationen speichern ("Zero Footprint").

Mobile Geräte, die von Safeguard-Personal genutzt werden, sind durch spezielle Profile geschützt, die nur mit einem Passwort zugänglich sind, das den Richtlinien entspricht, und/oder durch biometrischen Zugang und Multi-Faktor-Authentifizierung. Safeguard-Personal speichert keine Daten zu Kunden auf mobilen Geräten.

Der Sicherheitsbeauftragte überprüft zweimal im Jahr, ob alle Geräte korrekt gesichert sind.

2.3.2 Konfigurationsmanagement und Verteilung

Ein Inventar der genutzten mobilen Geräte wird in der Configuration Management Database (CMDB) geführt.

Wenn ein Gerät an einen Standort außerhalb des Arbeitsbereichs von Safeguard gebracht wird, muss eine Genehmigung vom Konfigurationsmanager eingeholt werden. Geräte außerhalb des Arbeitsbereichs müssen durch die oben genannten Maßnahmen gesichert werden.

Der Konfigurationsmanager ist verantwortlich für die Aktualisierung der CMDB, wenn sich etwas ändert, und wird die CMDB mindestens einmal alle drei Monate aktualisieren.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 6 von 36

3. Passwortrichtlinie und Kontozugriff

Bei Safeguard stellen wir sicher, dass alle Mitarbeiter ihre Konten und Passwörter korrekt verwenden. Es gibt verschiedene Verfahren, um dies zu gewährleisten:

3.1 Passwortrichtlinie

Alle Mitarbeiter sind verpflichtet, sichere Passwörter für alle Konten zu verwenden.

Die Passwortrichtlinie ist in allgemeine und spezifische Anforderungen unterteilt. Alle Konten müssen die Anforderungen beider Kategorien erfüllen. Anfangspasswörter und zurückgesetzte Passwörter haben eine maximale Gültigkeit von einem Geschäftstag und müssen bei der ersten Verwendung in ein Passwort geändert werden, das der Passwortrichtlinie entspricht.

Die allgemeinen Anforderungen sind unten aufgeführt:

- Passwörter müssen mindestens 4 von 5 Zeichentypen enthalten:
 - Kleinbuchstaben
 - Großbuchstaben
 - Zahlen
 - Satzzeichen (zum Beispiel: “;’?;!)
 - Symbole (zum Beispiel: @#\$%^&* <>~+=)
- Das Wiederverwenden desselben Passworts, wenn das Passwort geändert werden muss, ist verboten.
- Standard-Kontonamen und -Passwörter werden nach dem ersten Login geändert. Nach der Einrichtung eines Informationssystems dürfen Standard-Kontonamen und -Passwörter nicht mehr vorhanden sein.

Alle Konten müssen als spezifischer Kontotyp klassifiziert sein; diese Typen sind unten erklärt. Diese Konten müssen die Anforderungen erfüllen, die mit ihrem Typ verbunden sind. Diese Anforderungen gelten zusätzlich zu den allgemeinen Anforderungen:

Anwendung-Verwaltungskonto

- Beschreibung: Ein persönliches Konto zur Verwaltung von Anwendungen, die auf Systemen ausgeführt werden.
- Typ: persönlich (auf eine bestimmte Person zurückführbar)
- Passwortlänge: mindestens 15 Zeichen

Administrator-Konto

- Beschreibung: Ein persönliches Konto, das dem Benutzer vollständigen Zugriff mit Administratorrechten gewährt.
- Typ: persönlich (auf eine bestimmte Person zurückführbar)
- Passwortlänge: mindestens 15 Zeichen

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 7 von 36

Büroautomationskonto (OA-Konto)

- Beschreibung: Ein persönliches Konto, das Mitarbeitern ermöglicht, in einer Büroautomationsumgebung zu arbeiten.
- Typ: persönlich (auf eine bestimmte Person zurückführbar)
- Passwortlänge: mindestens 8 Zeichen

Für Informationssysteme, die unsere allgemeinen und spezifischen Passwortrichtlinien nicht erfüllen, muss eine Risikobewertung durchgeführt und erforderliche Maßnahmen ergriffen werden. Diese Anomalien werden dokumentiert und kommuniziert. (Sicherheits-Checkliste)

Wir verwenden 1Password als Passwort-Tresor. Der Sicherheitsbeauftragte ist verantwortlich für die korrekte Umsetzung der oben genannten Passwortrichtlinie über 1Password. Der Sicherheitsbeauftragte überprüft regelmäßig, ob die Mitarbeiter unsere Passwortanforderungen einhalten.

3.2 Multi-Faktor-Authentifizierung (MFA)

Wo möglich, wird MFA von den Systemen, die wir verwenden, erzwungen. Wenn eine Durchsetzung nicht möglich ist, müssen die Mitarbeiter MFA dennoch dort aktivieren, wo dies möglich ist. Wenn keine MFA verfügbar ist, muss eine Risikobewertung durch den Sicherheitsbeauftragten durchgeführt und dokumentiert werden.

MFA-Codes dürfen nicht in der von uns verwendeten Passwort-Manager-Software (wie in 4.3 beschrieben) gespeichert werden, sondern nach Möglichkeit in der Google Authenticator-App. Wenn die Authenticator-App nicht verwendet werden kann, darf SMS verwendet werden.

3.3 Kontozugriff

Mitarbeiter erhalten Zugang nach dem Prinzip „Need-to-Know“. Sie sollten nach Möglichkeit Single Sign-On (SSO) über Google verwenden, um die Anzahl der genutzten Konten zu reduzieren. (Sicherheits-Checkliste)

Wenn eine Person dem Unternehmen beitrifft, wird ihr gemäß Protokoll der entsprechende Zugriff gewährt. Ein ähnliches Protokoll gilt, wenn ein Mitarbeiter das Unternehmen verlässt.

Kontonamen dürfen keinen Hinweis auf das Zugriffslevel enthalten (zum Beispiel darf „Henk Administrator“ nicht verwendet werden).

Verschiedene Konten sollten für unterschiedliche Zugriffslevels genutzt werden. Widersprüchliche Rollen und Verantwortlichkeiten sollten separate Konten verwenden, um das Risiko von unbefugtem oder versehentlichem Ändern oder Missbrauch von Unternehmensressourcen zu minimieren.

Wer welchen Zugriff hat, wird in der Autorisierungsmatrix festgehalten. Der Sicherheitsbeauftragte überprüft dies zweimal im Jahr, um sicherzustellen, dass sie noch aktuell

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 8 von 36

ist. Der Sicherheitsbeauftragte überprüft auch zweimal im Jahr, ob die Zugriffslevels noch aktuell sind und ob ein Mitarbeiter keinen Zugriff auf Dienste hat, zu denen er Zugang haben sollte.

Wenn ein Mitarbeiter Zugang zu einem Dienst benötigt, zu dem er zuvor keinen Zugang hatte, wird folgendes Verfahren angewandt:

1. Der Mitarbeiter schickt eine Zugriffsanfrage an den Sicherheitsbeauftragten.
2. Der Sicherheitsbeauftragte führt dann eine Risikobewertung für die Zugriffsanfrage durch.
3. Wenn der Sicherheitsbeauftragte die Anfrage genehmigt, wird ein neues Konto für den Mitarbeiter erstellt. Dieses Konto sollte vorzugsweise ein temporäres Konto sein, abhängig von den tatsächlichen Anforderungen des Mitarbeiters und den damit verbundenen Sicherheitsrisiken.
 - a. Der Mitarbeiter erhält die notwendigen Informationen zum neuen Konto vom Sicherheitsbeauftragten.
 - b. Das Konto wird vom Eigentümer des IT-Assets erstellt.
 - c. Der Sicherheitsbeauftragte aktualisiert die Autorisierungsmatrix.
4. Wenn der Sicherheitsbeauftragte die Anfrage ablehnt, informiert er den Mitarbeiter über die Gründe für die Ablehnung.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 9 von 36

4. Sicherheit IT

Sicherheit ist ein wichtiger Bestandteil der Safeguard-Plattform, daher haben wir die in diesem Kapitel aufgeführten Maßnahmen eingeführt, um dies sicherzustellen.

4.1 DDoS-Schutz

Für den DDoS-Schutz verwenden wir AWS Shield Standard. Dies ist ein von AWS bereitgestellter DDoS-Schutzdienst, der die Anwendungen von Safeguard schützt. AWS Shield bietet kontinuierliche Erkennung und automatische Inline-Maßnahmen, die Ausfallzeiten und Latenzzeiten der Anwendungen minimieren.

4.2 Kryptografie

Wir verwenden TLS 1.2-Zertifikate für alle Client-Server-Kommunikation. Einmal im Jahr erneuern wir diese Zertifikate und aktualisieren sie auf eine neue TLS-Version, falls zutreffend.

Wir haben eine Richtlinie zur standardmäßigen Verschlüsselung und verwenden den Industriestandard, wo er verfügbar ist. Wir nutzen EBS Encryption von AWS in Kombination mit dem AWS Key Management Service (KMS).

4.3 Übertragung personenbezogener Daten

Wenn personenbezogene Daten an Kunden übertragen werden, erfolgt dies immer verschlüsselt. Das Passwort zum Entsperren der Daten wird immer über ein anderes Medium gesendet (zum Beispiel per SMS). Weitere Informationen zur Datenübertragung finden Sie in Abschnitt 9.2.

4.4 Penetrationstests (Pen-Testing)

Wir lassen einmal im Jahr einen externen Anbieter einen Black-Box-Penetrationstest (Pen-Test) am Safeguard-System durchführen. Wenn ein Pen-Test die Erfolgskriterien nicht erfüllt, beheben wir die schwerwiegenden und kritischen Feststellungen innerhalb von drei Monaten und führen innerhalb von drei Monaten nach der Behebung der Feststellungen einen neuen Pen-Test durch. Alle Pen-Test-Berichte werden im Safeguard-Dateisystem gespeichert und organisiert.

4.5 Datenvalidierung

Wir verlangen, dass alle eingehenden Daten validiert werden, indem geeignete Frameworks in unserem Code eingesetzt werden, um deren Integrität zu gewährleisten. Diese Validierung umfasst den Schutz vor Injection-Angriffen, die Überprüfung der Datentypen, das Entfernen ungültiger Zeichen, die Überwachung auf Werte außerhalb des zulässigen Bereichs und die Einhaltung vordefinierter Datenlimits.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 10 von 36

4.6 Malware, Härtung und Patchen

In der AWS-Umgebung nutzen wir bestehende Funktionen in Form von Diensten, die sicherstellen, dass die dort vorhandenen Workloads gemäß den festgelegten Anforderungen eingerichtet und konfiguriert sind.

Zunächst verwenden wir dafür AWS Config. Dieser Dienst stellt sicher, dass alles, was in einer AWS-Umgebung passiert, über eine festgelegte Liste von Anforderungen abgewickelt wird. Immer wenn diese Anforderungen nicht erfüllt werden, können automatische Maßnahmen ergriffen werden. Zum Beispiel könnte eine Anforderung sein, dass Systemprotokollinformationen an das richtige AWS-Konto gesendet werden. Sollte dies deaktiviert werden, kann AWS Config es automatisch wieder aktivieren. Auch die Systemhärtung wird auf diese Weise durchgesetzt.

Neben diesen Kontrollen verwenden wir Amazon Inspector, um zu prüfen, ob Workloads anfällig für bekannte Schwachstellen sind, und nutzen automatisierte Systeme, um Umgebungen auf das richtige Leistungsniveau zu bringen.

Für Anti-Malware verwenden wir eine renommierte Anti-Malware-Lösung, derzeit ist dies Trend Micro.

Wir nutzen NordLayer's 'ThreatBlock' als Webfilter.

Weitere Informationen finden sich auch in Kapitel 6.2.

4.7 Sicherheitsprüfungen

Zweimal im Jahr wird der Sicherheitsbeauftragte eine Sicherheitsprüfung durchführen. Diese Prüfung umfasst Folgendes:

1. Passwortprüfung bei Safeguard-Mitarbeitern, um sicherzustellen, dass die im Kapitel 3 beschriebene Richtlinie befolgt wird.
2. Physische Sicherheitsprüfung von Schlüsseln, um sicherzustellen, dass die im Kapitel 2 beschriebene Richtlinie befolgt wird.
3. Prüfung auf klare Schreibtische und klare Bildschirme, um sicherzustellen, dass die im Kapitel 12 beschriebene Richtlinie eingehalten wird.
4. Geräteprüfung, um sicherzustellen, dass Laptops und Mobiltelefone gemäß der im Kapitel 2 beschriebenen Richtlinie aktuell und gewartet sind.
5. Datenschutzprüfung, um sicherzustellen, dass keine persönlichen Daten auf Mitarbeiter-Laptops gespeichert sind.
6. Sicherstellen, dass die Autorisierungsmatrix aktuell ist.
7. Durchführen einer Protokollanalyse.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 11 von 36

5. Sicherheitsvorfälle

In diesem Kapitel wird erläutert, wie der Prozess für das Melden von Sicherheitsvorfällen funktioniert.

5.1 Vorfallmeldung

Wir haben einen 24/7-Vorfallmeldeprozess eingerichtet, um Kunden im Falle von Sicherheitsvorfällen zu benachrichtigen. Diese Vorfälle sollten an die vereinbarten Kundenkontakte gemeldet werden.

Der Vorfallmeldeprozess ist in der SLA, der Auftragsverarbeitungsvereinbarung und den allgemeinen Geschäftsbedingungen festgelegt, die zwischen Safeguard und dem Kunden abgeschlossen wurden.

Umgekehrt können Kunden Vorfälle, die sie selbst entdeckt haben, 24/7 melden. Diese Vorfälle umfassen, sind aber nicht beschränkt auf:

- Distributed Denial of Service (DDoS): Ein Angriff, der einen vertraglich vereinbarten Dienst für seine Nutzer unzugänglich macht, wobei die Quelle des Angriffs mehr als eine eindeutige IP-Adresse ist. DDoS-Tests sind in Kapitel 4.1 näher dokumentiert.
- Advanced Persistent Threat (APT): Eine Reihe von heimlichen und kontinuierlichen Computer-Hacking-Prozessen zur Überwachung oder Extraktion von Daten von einem bestimmten Ziel, das mit dem Dienst in Verbindung steht.
- Datenkorruption: Die absichtliche Einführung von nicht autorisierten Änderungen an Kundendaten.
- Datenleck: Die nicht autorisierte Übertragung von Kundendaten aus einer Organisation an ein externes Ziel oder einen externen Empfänger.
- Ransomware: Eine Form von Malware, die den Computer eines Benutzers als Geisel hält, bis eine „Lösegeldgebühr“ bezahlt wird.
- Geldbetrug: Die unrechtmäßige Nutzung von IT-Systemen des Kunden oder seines Dienstansbieters zur gezielten Täuschung, um unfaire oder illegale Gewinne zu erzielen. Geldbetrug umfasst Cyberverbrechen wie (großflächigen) elektronischen Identitätsdiebstahl oder unrechtmäßiges Eindringen in ein Netzwerk.

5.2 Vorfallbearbeitung

Wenn wir einen Sicherheitsvorfall identifizieren, informieren wir die betroffenen Parteien innerhalb von 24 Stunden. Wenn eine externe Partei (z.B. Kunden) einen Sicherheitsvorfall entdeckt, arbeiten wir mit dieser Partei zusammen, um den Vorfall so schnell wie möglich zu lösen.

Wir werden ein Nachbereitungstreffen mit den Entwicklungs- und Sicherheitsteams abhalten, um aus dem Vorfall und dem Prozess selbst Lehren zu ziehen, und die betroffenen Parteien über die

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 12 von 36

daraus gewonnenen Erkenntnisse informieren. Alle Faktoren in Bezug auf Vorfälle werden in einem Dokument protokolliert, basierend auf einer festgelegten Vorlage.

Die Sicherheitsvorfälle, zusammen mit den Lösungen dafür und den daraus gezogenen Lehren, werden im Sicherheitsvorfallprotokoll dokumentiert. Protokolle werden weiter in Kapitel 7 erläutert.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 13 von 36

6. Software-Updates und Entwicklung

In diesem Kapitel wird der Entwicklungsprozess der Safeguard-Plattform erläutert. Dieser Prozess wird durch die Versionshistorie und die Protokollierung auf den Plattformen Jira und GitHub abgesichert.

6.1 Entwicklungsprozess

Safeguard verwendet eine DTAP-Strategie (Development, Test, Acceptance, Production) mit physisch getrennten Umgebungen, um eine Dateninterferenz zu minimieren. Die Umgebungen werden auf AWS-Servern gehostet. Safeguard verwendet in allen Entwicklungsprozessen das Prinzip "Privacy by Design".

Wir nutzen JIRA als Projektmanagement-Tool und wenden eine Agile-Methodik an. Es gibt im Allgemeinen zwei Gründe, ein Ticket in JIRA zu erstellen:

1. Ein intern oder extern gemeldeter Fehler;
2. Die Entwicklung einer neuen Funktion oder die Aktualisierung und Verbesserung einer bestehenden Funktion.

Wenn ein Fehler gemeldet wird, bestimmt eine Folgenabschätzung, wie schnell er behoben werden muss, wobei die Priorität von kritisch bis niedrig reicht.

Die Idee für eine neue Funktion oder Verbesserung kann aus Kundenfeedback, Forschung oder internen Diskussionen stammen. Wenn die Idee bereit für die Design- und Entwicklungsphase ist, wird sie in JIRA verschoben und durchläuft die folgenden Schritte:

1. To-do im Design: Die Tickets, an denen ein Designer arbeitet;
2. Recherche: Der Designer und der Produktmanager sammeln Informationen;
3. Design: Der Designer erstellt ein erstes Konzept der Funktion und ihres Funktionsumfangs;
4. Überprüfung: Das Design wird von einem anderen Mitglied des Designteams überprüft;
5. Tickets für die Entwicklung erstellen: Der Designer erstellt Tickets für das Entwicklungsteam;
6. To-do in der Entwicklung: Das Ticket wartet darauf, dass ein Entwickler daran arbeitet;
7. In Arbeit: Ein Entwickler arbeitet am Ticket;
8. Code-Review: Jedes Ticket muss zuerst von mindestens einem anderen Entwickler überprüft und durch automatisierte Tests und andere Qualitätskontrollen genehmigt werden;
9. Test 1: Das Ticket wird von einem qualifizierten Mitglied des Testteams getestet;
10. Test 2: Ein weiteres Mitglied des Testteams wird dasselbe Ticket testen;

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 14 von 36

11. Getestet: Das Ticket wartet auf den Übergang von der Entwicklungsumgebung zur Abnahmeumgebung;
12. Qualitätssicherung (QA) 1: Das Ticket wird in der Abnahmeumgebung getestet;
13. QA 2: Das Ticket wird erneut von einem anderen qualifizierten Tester geprüft;
14. Warten auf Veröffentlichung: Wenn ein Ticket vollständig getestet wurde und die Tests bestanden hat, wird es auf die Veröffentlichung warten;
15. Veröffentlicht: Das Ticket wurde in der Produktionsumgebung veröffentlicht.

Zusätzlich zu den oben beschriebenen Schritten werden vor jeder neuen Veröffentlichung drei weitere unabhängige Tests durchgeführt:

- Ein Regressionstest, der jede Funktionalität des Produkts überprüft, um sicherzustellen, dass neue Änderungen andere Funktionalitäten nicht beeinträchtigt haben;
- Ein Abnahmetest, der nach Abschluss der Qualitätssicherungsphase durchgeführt wird. Dieser testet die kritischsten Funktionen des Produkts und ist der letzte Check vor der Veröffentlichung;
- Ein Veröffentlichungstest, der nach einer neuen Veröffentlichung durchgeführt wird, um sicherzustellen, dass sie in der Produktionsumgebung funktioniert.

Schritte 7 und 8 werden in der Entwicklungsumgebung durchgeführt, Schritte 9 und 10 werden in der Testumgebung durchgeführt, Schritte 12 und 13 werden in der Abnahmeumgebung durchgeführt und Schritt 15 erfolgt in der Produktionsumgebung.

Alle Testdaten werden mit Dummy-Testdaten erstellt. Keine persönlichen Daten von Kunden werden bei der Entwicklung oder dem Test verwendet.

Wenn während des Testprozesses ein Fehler gefunden wird oder das Ticket nicht wie beabsichtigt funktioniert, wird das Ticket abgelehnt und zurück in die „To-do in development“-Phase verschoben, unter einem neuen Bestandteil: Test fehlgeschlagen. Das Ticket durchläuft dann alle Schritte erneut, bis es für die Veröffentlichung bereit ist.

Die für das Testen verantwortlichen Mitarbeiter verfügen über tatsächliche, fachliche Kenntnisse, Fähigkeiten, Schulungen und Erfahrungen im Bereich Testen, Datenschutz und Sicherheit.

6.2 Abhängigkeiten von Drittanbietern, Patches und Schwachstellen

Wir bewerten jede Abhängigkeit anhand einer Checkliste. Diese Liste wird jährlich überprüft. Die Überprüfung jeder neu hinzugefügten Abhängigkeit ist Teil unseres Code-Review-Prozesses, der sicherstellt, dass jede Abhängigkeit nur hinzugefügt wird, wenn es angebracht ist. Für Abhängigkeiten, die von einem Lieferanten verwaltet werden, ist keine Risikobewertung erforderlich, da wir alle unsere Lieferanten gemäß den Vorgaben in Abschnitt 9.3 bewerten.

Wir verwenden Dependabot, um automatisch nach bekannten Schwachstellen und Patches in unseren Abhängigkeiten zu suchen und Pull-Requests zu erstellen, um diese zu beheben. Unser Sicherheitsbeauftragter wird automatisch benachrichtigt, wenn es größere Probleme gibt.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 15 von 36

Darüber hinaus überprüft bei jeder Veröffentlichung der leitende Entwickler für jede Plattform manuell alle Abhängigkeiten auf mögliche Patches oder Schwachstellen und aktualisiert sie entsprechend. Dies wird mittels des Formulars für Abhängigkeitskontrolle dokumentiert.

6.3 Veröffentlichungspolitik

Safeguard hat eine Veröffentlichungspolitik, die definiert, wann und wie Veröffentlichungen gehandhabt werden. Wichtige Veröffentlichungen werden gemäß unserem Entwicklungsfahrplan geplant. Wir halten jede Veröffentlichung so „klein“ wie möglich, um sicherzustellen, dass der Einfluss auf andere Funktionalitäten minimiert wird. Jede Veröffentlichung der App wird schrittweise eingeführt, enthält einen Backup-Plan und wird dokumentiert.

Eine Funktionsanforderung oder ein Verbesserungsvorschlag wird vom Auftragnehmer bewertet, und der Einreicher wird über das Ergebnis dieser Bewertung informiert. Wenn die angeforderte Funktionalität oder der Verbesserungsvorschlag implementiert wird, wird der Einreicher auch darüber informiert, in welcher Veröffentlichung (Minor Release oder Major Release) sie verfügbar sein wird.

Die Veröffentlichungspolitik von Safeguard basiert auf Auswirkung und Umfang und ist in drei verschiedene Veröffentlichungstypen unterteilt:

- Major Release: eine wichtige Einführung von Funktionen mit einer erheblichen Erweiterung der Funktionalität. Diese Veröffentlichungen bieten oft Lösungen für eine Reihe bekannter Fehler, Workarounds und schnelle Korrekturen. Diese Veröffentlichungen werden als Version 1, Version 2 usw. identifiziert.
- Minor Release: eine Einführung geänderter Funktionen mit Veränderungen in der Funktionalität und Verbesserungen für bekannte Fehler, Workarounds und schnelle Korrekturen. Diese Veröffentlichungen werden oft als Version 1.1, Version 2.1 usw. bezeichnet.
- Patch Release: eine Reihe von nicht-funktionalen Änderungen und geringfügigen Verbesserungen für bekannte Fehler, Workarounds und schnelle Korrekturen. Diese Veröffentlichungen werden oft als Version 1.1.1, Version 2.1.2 usw. bezeichnet.

Für jede Veröffentlichung dokumentiert der CTO die Veröffentlichung mit einem spezifizierten Formular.

Bei größeren Veröffentlichungen informieren die Funktionsmanager die Kunden vor der Veröffentlichung über die Änderungen in der Veröffentlichung und bieten ihnen nach Bedarf nach der Veröffentlichung Schulungen an.

6.4 Quellcode und technische Dokumentation

Der gesamte Quellcode und die technische Dokumentation unterliegen der GIT-Versionskontrolle auf Github und befinden sich niemals in einer Produktionsumgebung.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 16 von 36

Entwickler erhalten nach dem Need-to-Know-Prinzip Zugriff, gemäß der in Kapitel 3.3 beschriebenen Kontozugriffsrichtlinie.

6.5 Risikobewertung

Eine Risikobewertung in Bezug auf das Safeguard-System wird vom Sicherheitsbeauftragten durchgeführt, wenn:

- Der Umfang des Systems erweitert wird, um neue Informationsressourcen mit neuen Funktionen einzubeziehen; und
- Eine neue Benutzergruppe eingeführt wird; oder
- Andere größere Änderungen die funktionalen und nicht-funktionalen Anforderungen beeinflussen, die eine Risiko- und Auswirkungenanalyse rechtfertigen.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 17 von 36

7. Protokollierung

Ereignisse innerhalb der Safeguard-Systeme werden in Form von Protokolldateien in einer Audit-Trail aufgezeichnet. Protokolldateien werden zur Problemidentifikation, zum Erkennen von Systemmissbrauch, zur Problemuntersuchung und zur Fehlerbehebung verwendet.

Audit-Trails müssen den Anforderungen der ISO/IEC 27001 und ISO 27701 entsprechen, um Integrität, Verfügbarkeit und Vertraulichkeit zu gewährleisten.

7.1 Rollenverteilung und Verantwortlichkeit

Um den Protokollierungsprozess von Safeguard zu steuern, wurden Rollen für die Überwachung von Protokolldateien, technische Forschung, funktionale Forschung, Überprüfung der Sicherheitsanforderungen und eine Rolle des Eigentümers eingerichtet, der letztlich für das System verantwortlich ist.

Log-Manager

Im Protokollsystem von Safeguard ist der Log-Manager für die Verwaltung und Überwachung des Protokollsystems verantwortlich. Der Log-Manager gilt als verantwortlich für das Protokollsystem.

Sicherheitsbeauftragter

Im Protokollsystem von Safeguard ist der Sicherheitsbeauftragte für die Untersuchung möglicher Sicherheitsbedrohungen und die Benachrichtigung der entsprechenden Personen im Falle einer Bedrohung verantwortlich.

Funktionsmanager

Der Funktionsmanager führt Untersuchungen im funktionalen Bereich durch. Bei Safeguard ist dies die Person, die den Kontakt zu den Kunden pflegt.

Technischer Manager

Der technische Manager führt technische Untersuchungen im Falle eines Vorfalls durch. Die erforderlichen Informationen werden vom Sicherheitsbeauftragten bereitgestellt.

7.2 Protokollverwaltung

7.2.1 Protokolldateistruktur

Um ausreichend Informationen über ein Ereignis zu sammeln, muss eine Protokolldatei mit Informationen über den Zeitpunkt, den Ort, die Ursache und den Inhalt des Ereignisses versehen werden. Hierbei werden die 4 W's (Wer, Was, Wo, Wann) verwendet. Detaillierte Informationen finden Sie in Tabelle 1.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 18 von 36

Tabelle 1: Anforderungsmatrix für Protokolldateien

	Beschreibung	Enforderlich
Wann	Zeit & Datum	Ja
Wo	Systemname	Ja
	System-IP-Adresse	Ja
	Systemversion	Optional
	Dienstname, Protokoll und Port	Optional
	Verwendetes Modul	Optional
Was	Ereignisbeschreibung	Ja
	Ereignisergebnis	Ja
	Eindeutige Kennung	Ja
Wer	Quelle (IP-Adresse, E-Mail, Telefon usw.)	Ja
	Benutzerkennung	Optional

Diese Informationen können verwendet werden, um potenzielle Probleme zu beheben. Wenn ein Kunde Kontakt aufnimmt, können wir die Informationen in den Prüfprotokollen verwenden, um Anfragen zu beantworten oder Ursachenuntersuchungen durchzuführen. Diese Informationen werden niemals an Kunden weitergegeben.

7.2.2 Zu protokollierende Ereignisse

Ereignisse werden automatisch protokolliert, wo immer dies möglich ist. Speziell im Safeguard-System wird ein Audit-Log-Modul verwendet, das wie in Kapitel 7.2.1 beschrieben strukturiert ist.

Wenn es nicht möglich ist, automatische Protokollierung innerhalb eines Systems zu verwenden, kann beispielsweise ein Logbuch von Administratoren verwendet werden. Manuell protokollierte Vorgänge werden innerhalb des Safeguard-Systems gespeichert.

Ereignisse, die mindestens in den Protokolldateien im Audit-Trail enthalten sind, sind:

- Verwendung von technischen Verwaltungsfunktionen. Beispiele hierfür sind die Änderung einer Konfiguration, das Ausführen von Systembefehlen und das Durchführen eines Backups oder einer Systemwiederherstellung.
- Verwendung von funktionalen Verwaltungsfunktionen. Beispiele hierfür sind die Freigabe neuer Funktionalitäten und Eingriffe in Datenbanken.
- Sicherheitsmanagementoperationen. Beispiele hierfür sind die Anpassung von Rechten und die Ausgabe (oder Einziehung) von Schlüsseln.

- Sicherheitsvorfälle. Beispiele hierfür sind fehlerhafte Anmeldeversuche und unberechtigte Nutzung von Systemfunktionalitäten.
- Störungen in einem System. Beispiele hierfür sind die Nichtverfügbarkeit von Diensten und das Erreichen der Serverkapazitätsgrenze.
- Aktionen von Benutzern. Beispiele hierfür sind Anmeldeversuche (sowohl korrekte als auch inkorrekte), Änderungen am Safeguard-System und Zugriff auf Dateien.

7.2.3 Ereignisse außerhalb des Protokollbereichs

Der Zweck der Protokollierung besteht darin, Ereignisse zu identifizieren und die Ursache des Geschehenen zu untersuchen. Die folgenden Daten sollten nicht in einer Protokolldatei enthalten sein:

- Datenschutzempfindliche Daten, die nicht erforderlich sind, um diese Aufgabe auszuführen.
- Sicherheitsempfindliche Daten wie: Passwörter, Verschlüsselungscodes, Zugangscodes, Einwahlnummern usw.
- Missbrauchsempfindliche Daten wie Kreditkartennummern und Bankkonten.

7.2.4 Schutz der Protokolldateien

Protokolldateien sind vor Fälschung und unbefugtem Zugriff geschützt. Alle Protokolldateien werden in einem separaten AWS-Konto gespeichert. Diese Dateien werden automatisch nach 90 Tagen gelöscht. Wenn ein Vorfall vermutet wird, werden die betroffenen Protokolldateien mindestens 3 Jahre lang gespeichert. Dies gewährleistet, dass Protokolldateien innerhalb des Zeitraums verfügbar sind, in dem eine Protokollanalyse für erforderlich gehalten wird.

Die Einsicht in Protokolldateien ist autorisierten Benutzern vorbehalten; diese Benutzer können nur die Protokolldateien anzeigen und nicht verändern oder löschen. Protokolldateien im Safeguard-System dürfen nicht geändert werden.

Eine Übersicht über aktuelle Berechtigungen finden Sie in unserer Berechtigungsmatrix.

Es gibt Überprüfungen für die Speicherung des Audit Trails. Wenn die Speicherkapazität der Datenbank für die Protokolldateien unter ein bestimmtes Limit fällt, führt dies zu automatischen Alarmen an den Log-Manager und den Sicherheitsbeauftragten. Selbst wenn der Protokollserver nicht erreichbar ist (oder die Dateispeicherung nicht mehr möglich ist), werden sie automatisch benachrichtigt.

7.2.5 Zeitsynchronisation

Es ist notwendig, die Systemzeit relevanter Informationssysteme zu synchronisieren, um Protokolldateien auf den verschiedenen Systemen zuverlässig analysieren zu können. Alle relevanten Informationsverarbeitungssysteme werden daher mit einem NTP-Server synchronisiert. Der Amazon Time Sync Service wird dafür verwendet.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 20 von 36

7.3 Berichterstattung und Überwachung

7.3.1 Berichterstattung

Berichte werden bei jeder Sicherheitsüberprüfung mithilfe einer Vorlage erstellt. Protokolldateien von Administratoren haben unter normalen Umständen (keine kritischen Nachrichten) die höchste Priorität, wenn Protokolldateien im Safeguard-System analysiert werden. Berichte bestehen aus einer Analyse der Situation, der Untersuchung der Ursache und, soweit möglich, einem Vorschlag für eine Lösung oder Maßnahmen.

7.3.2 Überwachung

Aktive Überwachung wird auf folgende Punkte angewendet (siehe Kapitel 4):

- Berichte, die Probleme in Live-Umgebungen verursachen. Hierfür wurden Auslöser eingerichtet, die von AWS und Updown.IO generiert werden. Warnungen werden direkt an das zuständige Personal kommuniziert.
- Bedrohungen wie:
 - DDoS-Angriff (siehe Kapitel 4.1)
 - Viren- oder Malware-Benachrichtigungen
 - Änderungen an Protokolldateien
 - Speicherkapazität
 - Unberechtigter Zugriff

7.3.3 Verteilung

Um auf gemachte Benachrichtigungen reagieren zu können, wurden Aufgaben für die Personen pro Rolle zugeordnet (siehe Tabelle 2). Innerhalb von Safeguard werden alle Arten von Bedrohungsmeldungen gleich behandelt. Berichte, die nicht als Bedrohung wahrgenommen werden, werden vom Protokollmanager überwacht und bei Bedarf vom Sicherheitsbeauftragten eskaliert.

Tabelle 2: Rollenbewertungen für die Protokollierung

Bedrohungstyp	Protokollmanager	Sicherheitsbeauftragter	Technischer Manager	Funktionsmanager
Bedrohungen	Bedrohungen erkennen und Sicherheitsbeauftragten informieren	Sicherheitsprobleme untersuchen	Untersuchen und lösen	Auswirkungen untersuchen und gegebenenfalls Endbenutzer informieren
Keine Bedrohungen	Überwachung und regelmäßige Überprüfung	Wenn ein Problem gefunden wird; Sicherheitsprobleme untersuchen.	Wenn ein Bericht ein technisches Problem ist; untersuchen und lösen.	Wenn ein Bericht ein funktionales Problem ist; Lösung untersuchen und ermitteln.

8. Backup und Wiederherstellung

Alle physischen Systeme befinden sich in sicheren Rechenzentren von Amazon Web Services (AWS), die den höchsten Qualitäts- und Sicherheitsstandards entsprechen und ISO 27001-konform sind.

Es wird alle 24 Stunden ein Backup erstellt. Diese Daten werden für 7 Tage gespeichert.

Innerhalb unserer AWS-Umgebung gibt es einen Unterschied zwischen Konten, die Zugriff auf verschiedene Systeme haben. Pro AWS-Konto wird entschieden, was auf der Grundlage des "Least-Privilege"-Prinzips getan werden kann und was nicht. Dies gilt für Benutzer, Benutzergruppen und Rollen, die das AWS-System verwenden kann. Alle Backup-Daten werden in einem separaten Konto platziert, dessen Zugriff streng reguliert ist. Der Zugriff auf diese Daten ist nur für autorisiertes Personal möglich.

Wir werden dieses Wiederherstellungsverfahren jedes Jahr oder bei wesentlichen Änderungen testen, um die Zuverlässigkeit im Notfall zu gewährleisten. Unser Sicherheitsbeauftragter ist für dieses Verfahren verantwortlich und wird ein spezifisches Formular verwenden. Ein Testbericht wird erstellt und archiviert, damit wir sicherstellen können, dass das richtige Verfahren befolgt wird.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 22 von 36

9. Verarbeitung personenbezogener Daten

Personenbezogene Daten innerhalb von Safeguard werden auf Servern in der EU, Irland, gespeichert und der Backup-Speicherort befindet sich in Deutschland, EU. Safeguard folgt den Richtlinien der DSGVO bei der Verarbeitung personenbezogener Daten. Verarbeitervereinbarungen werden in Absprache mit Kunden erstellt und unterzeichnet.

Die Kunden bleiben die Eigentümer der auf der Safeguard-Plattform generierten Daten. Mitarbeiter von Safeguard dürfen diese personenbezogenen Daten nur für den vorgesehenen Zweck verarbeiten. Der Zugriff auf diese personenbezogenen Daten wird protokolliert. Dateien, die zwischen Safeguard und Kunden ausgetauscht werden und personenbezogene Daten enthalten, werden verschlüsselt.

Mitarbeiter von Safeguard, die berechtigt sind, personenbezogene Daten zu verarbeiten, verfügen über eine gültige "VOG" (Verklaring Omtrent Gedrag - Erklärung zum Verhalten). Diese wird im Personalordner aufbewahrt.

9.1 Klassifizierung von Benutzerdaten

Safeguard speichert Benutzerdaten, um korrekt zu funktionieren. Diese Daten gelten als persönlich und klassifiziert. Die Bewertung der Klassifizierung wird jährlich vom Datenschutzbeauftragten überprüft.

- Name - Bis zur Vertragsbeendigung
- E-Mail-Adresse - Bis zur Vertragsbeendigung
- Telefonnummer - Bis zur Vertragsbeendigung
- Funktion - Bis zur Vertragsbeendigung
- Allgemeine Telefon-Hardwareinformationen (Marke und Typ) - 90 Tage
- Telefon-Einstellungen (Push-Benachrichtigungen, GPS, WLAN, Betriebssystemversion und App-Version) - 90 Tage
- Anwesenheit von Benutzern an vordefinierten Orten - 90 Tage
- Daten zur Erstellung von und Reaktionen auf Alarme - 90 Tage
- Prüfprotokolle - 90 Tage
- Profilbilder - Bis zur Vertragsbeendigung
- Protokolldateien, die zur Problemlösung und Unterstützung verwendet werden - 90 Tage
- Konversationen mit unserem Support-Team über die In-App-Chat-Funktion oder per E-Mail - Bis zur Vertragsbeendigung

Wir erfassen diese Daten zu folgenden Zwecken:

- Um unsere Dienstleistungen zu liefern und zu personalisieren.
- Um Benutzer über unsere Produkte und Dienstleistungen zu informieren.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 23 von 36

- Zur Finanzverwaltung.

Daten, die bis zur Vertragsbeendigung gespeichert werden, werden bei Beendigung gelöscht.
Daten, die 90 Tage lang gespeichert sind, werden automatisch gelöscht.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 24 von 36

9.2 Ausstiegsstrategie

Hinsichtlich des Ausstiegsplans, den Safeguard verwendet, wird Folgendes angenommen:

1. Mit Beendigung des Nutzungsvertrags läuft die Option zur Nutzung der Safeguard-App ab.
2. Die Bedingungen für die Nutzung der Safeguard-App sind im Vertrag festgelegt, der mit dem betroffenen Kunden abgeschlossen wurde.
3. Der von Safeguard verwendete Ausstiegsplan gilt sowohl bei Ablauf des Vertrags als auch in Fällen, in denen der Vertrag möglicherweise nicht abgelaufen ist, aber die Beziehung zu Safeguard als Auftragnehmer aus irgendeinem Grund endet.
4. Der Betrieb eines abgeschlossenen Verarbeitervertrags gilt bis zum Zeitpunkt, an dem die Durchführung des Ausstiegsplans abgeschlossen ist. In der Praxis bedeutet dies, dass die Daten übertragen wurden.
5. Beim Bereitstellen der Daten wird Safeguard gemäß dem Ausstiegsplan eine Übersicht hinzufügen, die zur Überprüfung der Vollständigkeit der Datenübertragung verwendet werden kann. In Absprache mit dem Kunden wird Safeguard zu Beginn der Beziehung festhalten, welche Daten von Safeguard verarbeitet und gespeichert werden und wie die Vollständigkeit dieser Daten im Falle eines Ausstiegs überprüft werden kann.
6. Safeguard kann die mit der App verarbeiteten und generierten Daten auf Wunsch zur Verfügung stellen. Safeguard verwendet JSON als Standardformat. Safeguard stellt dem Kunden die Daten ab 90 Tage vor dem Ablaufdatum des Vertrags zur Verfügung.
7. Der Kunde erhält alle Daten bei Bereitstellung.
8. Der Ausstiegsplan wird innerhalb von maximal 30 Tagen nach Beendigung des Nutzungsvertrags abgeschlossen.

9.3 Unterauftragnehmer

Safeguard verwendet Unterauftragnehmer, um unseren Kunden den Service bereitzustellen. Unterauftragnehmer, die personenbezogene Daten verarbeiten, müssen nachweislich über ISO 27001- oder SOC-II-Zertifizierungen verfügen oder vergleichbare dokumentierte Prozesse haben. Wir betrachten ISO 27001 oder SOC II als Branchenstandard und daher ausreichend. Zertifikate oder Managementaussagen von Unterauftragnehmern, die personenbezogene Daten verarbeiten, müssen jährlich vorgelegt werden. Elektronische Nachrichten, die zwischen Unterauftragnehmern und Safeguard ausgetauscht werden, sind gemäß den Richtlinien in Kapitel 10 verschlüsselt.

Safeguard muss mit allen Unterauftragnehmern, die Benutzerdaten verarbeiten, eine Verarbeitungsvereinbarung haben.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 25 von 36

10. Business Continuity Management (BCM)

Safeguard verfügt über Kontinuitätspläne, in denen Maßnahmen ergriffen wurden, um Unterbrechungen der Dienste für die Kunden in den kritischen Serviceprozessen zu verhindern. Dies schützt sie vor den Folgen schwerwiegender Ausfälle und stellt sie wieder her. Dies garantiert auch die Kontinuität der Informationssicherheit. Diese Pläne werden jährlich überprüft und gegebenenfalls verfeinert und mit Kunden kommuniziert, die dies wünschen.

10.1 IT-Service-Kontinuitätsmanagement

Safeguard hat eine Entscheidungsstruktur und Organisation für eine schnelle Wiederherstellung im Notfall eingerichtet (siehe Tabelle 3). Im Falle eines schwerwiegenden Notfalls liegt ein Wiederherstellungsplan und ein Notfallplan vor.

Tabelle 3: Kriseneskalationsmatrix

Rolle	Normal	Krise
Führungsgremium	• Bestimmen der BCM-Richtlinie und -Strategie • Personalmanagement • Bestimmen des Zugangs zu Prozessen	• Krisenmanagement • Externer Kontakt
Management	• Prozessmanagement • Kommunikation und Bewusstsein • Integration von ITSCM in BCM • Durchführung einer Risikoanalyse • Produkte definieren • Verträge erstellen • Tests durchführen	• Koordination • Prozesskontrolle • Ressourcen bereitstellen • Beginn von Kontinuität und Wiederherstellung • Teamleitung • Bericht
Mitarbeiter	• Produkte entwickeln • Verhandeln • Tests durchführen • Berichte erstellen • Verfahren entwickeln	• Wiederherstellung durchführen • Teamarbeit

"Unser Hosting-Partner AWS wendet seinen eigenen Business Continuity Management-Prozess an, gefolgt von einem IT-Service Continuity Management-Prozess."

10.2 Treuhandvertrag

Im Interesse der Kontinuität des Dienstes hat Safeguard eine Cloud-Secure-Vereinbarung getroffen, die von Kunden gegen Gebühr genutzt werden kann. Die Cloud-Secure-Vereinbarung ermöglicht es dem Kunden, den Dienst im Falle eines Konkurses von Safeguard ohne Ausfallzeit für ihren Dienst weiterhin zu nutzen.

Safeguard verfügt über eine redundante Rechtsstruktur durch verschiedene juristische Personen, in denen das geistige Eigentum des Dienstes vom Betriebsunternehmen getrennt ist.

Im Falle eines Konkurses der Intellectual Property B.V. tritt die Cloud-Secure-Vereinbarung für Kunden in Kraft, die sie erworben haben. Die Kontinuität des Dienstes wird dann durch die Safeguard Secure Foundation garantiert, die den Dienst nur unter vorher festgelegten Bedingungen fortsetzen kann.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 27 von 36

11. Personal

Bei Safeguard legen wir großen Wert auf unser Personal und die Sicherheit der Daten unserer Kunden. Daher haben wir Verfahren, die erklären, wie unser Personal überprüft und geschult wird. Diese Verfahren finden Sie in diesem Kapitel.

11.1 Überprüfung

Safeguard führt einen Überprüfungsprozess durch, wenn neues Personal eingestellt wird. Das Personal von Safeguard hat eine VOG, die nicht älter als 3 Jahre ist. Jedes Jahr überprüft der Personalmanager, welche VOGs ablaufen und ob sie noch gültig sind. Wir haben ein Kontrollformular, um diese Überprüfung durchzuführen.

11.2 Schulung

Jedes Jahr bietet der Sicherheitsbeauftragte von Safeguard Schulungen an, die der Art der auszuführenden Arbeit angemessen sind und mindestens auch die persönliche Verantwortung umfassen. Spezifische Anforderungen in Bezug auf Sicherheitsframeworks von Kunden werden in den nächsten Schulungen enthalten sein.

Ein Teil dieser Schulung ist das Aufklärungsprogramm für Verhaltensaspekte sicheren mobilen Arbeitens und alle anderen Fragen im Zusammenhang mit Kontosicherheit und Datenschutz. Alle Mitarbeiter sind verpflichtet, ein unterschriebenes Formular einzureichen, in dem sie bestätigen, dass sie die Schulung absolviert haben.

Der Arbeitsvertrag der Mitarbeiter enthält eine Bestimmung für mobiles Arbeiten, durch die sie erklären, dass sie sich der Gefahren des mobilen Arbeitens bewusst sind und dies sicher tun werden.

Mitarbeiter unterzeichnen eine Benutzervereinbarung für die Arbeit auf mobilen Geräten, in der sie erklären, dass sie sich der Gefahren der (fernen) Arbeit auf mobilen Geräten bewusst sind und dies sicher tun werden. Diese Vereinbarung gilt für alle mobilen Geräte, die der Mitarbeiter für geschäftliche Aktivitäten verwendet.

11.3 Vertraulichkeit

Mitarbeiter von Safeguard und Unterauftragnehmer unterzeichnen eine Geheimhaltungsvereinbarung. In dieser Vertraulichkeitserklärung sind folgende Punkte enthalten:

- Die Beziehung zwischen den Parteien;
- Der Grund, warum vertrauliche Informationen bereitgestellt werden;
- Auf welche vertraulichen Informationen sich die Erklärung bezieht;

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 28 von 36

- Welche Konsequenzen (möglicherweise) eintreten, wenn die empfangende Partei gegen die Vertraulichkeitserklärung verstößt;
- Ob die empfangende Partei Mitarbeiter hat. Die empfangende Partei muss auch diese Mitarbeiter an die Vertraulichkeitserklärung binden.
- Strafklausel.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 29 von 36

12. Sicherheitsrichtlinie

12.1 Von Vision, Mission bis Strategie

12.1.1 Dienstleistungen

Safeguard B.V. bietet folgende Dienstleistungen an: Die Safeguard-App, eine Anwendung zur Alarmierung von Rettungskräften und zur Kommunikation während eines Vorfalls.

- Wir bieten diese Dienstleistungen folgenden Kunden (Gruppen) an: Organisationen und Unternehmen mit einer Notfallorganisation von mindestens 5 Notfallbeauftragten.
- Umfang der Dienstleistung: Entwicklung, Implementierung, Management und Unterstützung der Safeguard-Cloud-Software zur Unterstützung von Notfällen.

12.1.2 Mission und Vision

Unsere Mission ist es, die richtigen Personen im Notfall zu alarmieren, damit sie Hilfe leisten können. Dies erreichen wir durch das Design, die Entwicklung und den Verkauf unserer Safeguard-App. Benutzerfreundlichkeit, Skalierbarkeit und Zuverlässigkeit sind unsere Leitwerte, die wir als Kompass verwenden, um weitere Schritte in unserem Unternehmen zu bestimmen.

Unsere Vision ist es, ein globales Netzwerk von Notfallhelfern zu schaffen, die im Notfall alarmiert werden können, um Hilfe zu leisten.

12.1.3 Kernwerte

Wir haben folgende Kernwerte:

- Die Integrität unserer Dienstleistungen ist wesentlich. Die Richtigkeit der Informationen, die innerhalb unserer Anwendung und innerhalb der Organisation verarbeitet werden, ist für uns von großer Bedeutung.
- Informationen werden gemäß unserer Informationssicherheitsrichtlinie und -protokollen behandelt.
- Die Benutzererfahrung unserer Anwendung ist für uns und unsere Kunden von großer Bedeutung.
- Die Skalierbarkeit unseres Dienstes ist wichtig, um unsere Vision zu verwirklichen.
- Die Zuverlässigkeit unseres Dienstes ist entscheidend, da unsere Kunden darauf angewiesen sind, dass Safeguard während eines Vorfalls ordnungsgemäß funktioniert. Unsere ICT-Infrastruktur ist redundant aufgebaut.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 30 von 36

12.2 Vom Strategie zur Richtlinie

12.2.1 Ort der Information und Datenschutz

Sicherheit und Datenschutz in der Strategie Informationsflüsse innerhalb von Safeguard B.V. haben fast immer mit der Verfügbarkeit, Integrität und Vertraulichkeit von datenschutzsensiblen persönlichen oder geschäftlichen Daten zu tun. Es ist daher sehr wichtig für Safeguard B.V., sicherzustellen, dass diese Daten ordnungsgemäß und angemessen gesichert sind und dass nur diejenigen Personen Zugang zu den Daten haben, die aufgrund ihrer Rolle die Daten für die weitere Arbeitsleistung verwenden müssen. Dies trägt erheblich zur Zufriedenheit unserer Kunden bei. Informationssicherheit und Datenschutz unterstützen unsere Mission, Vision und unsere Kernwerte: Wir streben eine kontinuierliche Verbesserung der Qualität unserer Dienstleistungen und Prozesse sowie der Informationssicherheit unserer Daten durch den Plan-Do-Check-Act-Zyklus an.

- Informationssicherheit und Datenschutz unterstützen unsere strategischen Ziele:
 - Die Ziele im Bereich Qualität, Datenschutz und Informationssicherheit von Safeguard B.V. unterstützen die Verwirklichung der Richtlinienziele. Die Ziele des vergangenen Jahres werden jährlich bewertet und die neuen Ziele für das kommende Jahr formuliert.

Wie bereits erwähnt, haben wir vier strategische Ziele:

- Relevanz für unsere Kunden haben;
 - Ausreichende Rentabilität, um Investitionen tätigen zu können;
 - Ausreichende Skalierung, um die Kontinuität zu gewährleisten;
 - Genügend Kunden, um das Risiko des Scheiterns zu überwinden. Die folgenden Informationen beziehen sich auf Sicherheitsziele: das Wiederherstellungszeitziel (RTO) beträgt 4 Stunden und das Wiederherstellungspunktziel (RPO) beträgt 28 Stunden.
-
- Informationssicherheit und Datenschutz unterstützen unsere Wettbewerbsstrategie:
 - Wir gewinnen das Vertrauen unserer Kunden, weil wir bestrebt sind, die Erwartungen der Kunden zu erfüllen oder zu übertreffen und ein optimales Gleichgewicht in Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Daten zu gewährleisten.
 - Wir sind konform mit den Anforderungen von Gesetzen und Regulierungsbehörden wie der Datenschutz-Grundverordnung (DSGVO).
 - Informationssicherheit und Datenschutz sind wesentlich in unserer Wettbewerbsstrategie, weil Safeguard B.V. eine Produktführung in Kombination mit einer Kundenintimitätsstrategie verfolgt. Es ist wichtig, dass alle Informationen zur Sicherheit und zum Datenschutz in Ordnung sind, um weiterhin das beste Produkt liefern zu können. Wenn Sicherheits- oder Datenschutzvorfälle auftreten, geht dies zu Lasten des Kundenvertrauens und wir sind weniger in der Lage, unsere Kundenintimitätsstrategie umzusetzen.
 - Qualität, Datenschutz und Informationssicherheit unterstützen unsere Wertschöpfungskette:

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 31 von 36

- Wir legen Prozesse klar, zielorientiert und transparent fest und stellen sicher, dass Informationen verfügbar, ehrlich und vertraulich sind.
- Wir strukturieren unsere Qualitäts- und Informationssicherheitsprozesse in einem formellen Managementsystem.
- Wir zertifizieren unser Managementsystem gemäß den Standards ISO 27001:2022, ISO 27701:2019 und ISO 9001:2015.

12.2.2 Konkrete Richtlinienpunkte

Allgemeine Richtlinie

Unsere allgemeinen Richtlinien lauten wie folgt:

- Wir arbeiten gemäß etablierten ISO-Prozessen.
- Wir arbeiten und kommunizieren transparent mit unseren Kunden und verfolgen einen unkomplizierten Ansatz.
- Wir haben einen Compliance-Beauftragten, einen Qualitätsmanager, einen Datenschutzbeauftragten und einen Sicherheitsbeauftragten ernannt, um unser Managementsystem zu unterstützen und zu koordinieren.
- Wir haben extern einen Datenschutzbeauftragten eingestellt, um Wissen und Fachkenntnisse zu nutzen.

Quality policy

Unsere Qualitätsrichtlinie konzentriert sich auf folgende Aspekte:

- Wir verwenden eine Kompetenzmatrix und stellen gut ausgebildetes Personal ein, das über die erforderlichen Zertifizierungen verfügt.
- Es gibt kontinuierliche Schulungen und persönliche Ziele für jeden Mitarbeiter, um sich in ihrem Bereich weiterzuentwickeln.
- Es gibt Kundenzufriedenheitsumfragen und andere Feedback-Mechanismen, um unsere Dienstleistungen zu verbessern.
- Ein umfangreicher Testplan wird im Entwicklungsprozess verwendet. Die Tests werden von verschiedenen Personen durchgeführt und durchlaufen mehrere Phasen. Nachdem Tickets in Test 1, Test 2 und QA genehmigt wurden, wird ein umfangreicher Systemtest durchgeführt.
- Es wird immer bewertet, ob eine gewünschte / angeforderte Funktion einen Mehrwert für das System darstellt und wird vor jeder Entwicklung bewertet, ob mit der Entwicklung begonnen wird.

Informationssicherheitsrichtlinie

Unsere Informationssicherheitsrichtlinie konzentriert sich auf die folgenden Aspekte:

- Als Vorstand unterstützen wir aktiv die Informationssicherheit innerhalb der Organisation, indem wir klare Richtlinien festlegen, Engagement zeigen und Verantwortlichkeiten für die Informationssicherheit ausdrücklich anerkennen und zuweisen. Aufgaben, Verantwortlichkeiten und Befugnisse sind in unseren Stellenbeschreibungen festgelegt, auf die wir in Kapitel 1 unseres integrierten Managementhandbuchs verweisen.
- Wir haben Richtlinien festgelegt, um den Austausch von Informationen durch die Nutzung aller Arten von Kommunikationseinrichtungen zu schützen.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 32 von 36

- Wir haben Zugriffsrichtlinien auf der Grundlage von Geschäfts- und Sicherheitsanforderungen für den Zugriff festgelegt, dokumentiert und bewertet.
- Wir haben eine "klare Schreibtisch"-Richtlinie für Papier und entfernbare Speichermedien und eine "klare Bildschirm"-Richtlinie für IT-Einrichtungen. Spezifische Vereinbarungen dazu sind in unserem HR-Informationssicherheitsprotokoll und in unserem Verhaltenskodex festgelegt.
- Im Hinblick auf die Nutzung von Netzwerkdiensten ist unser Ausgangspunkt, dass Benutzern nur Zugriff auf Dienste gewährt wird, für die sie ausdrücklich autorisiert sind. Detaillierte Vereinbarungen zu Netzwerkdiensten sind in unserem Informations-sicherheitsprotokoll für das ICT-Management festgelegt.
- Wir haben eine strenge Richtlinie zum Schutz vor Risiken im Zusammenhang mit der Nutzung von tragbaren Computern und Kommunikationseinrichtungen. Einzelheiten dazu sind sowohl in unserem Facility Management-Informationssicherheitsprotokoll als auch in unserem Verhaltenskodex festgelegt.
- Wir haben eine strenge Richtlinie für die Telearbeit. Einzelheiten dazu sind sowohl in unserem Facility Management-Informationssicherheitsprotokoll als auch in unserem Verhaltenskodex festgelegt.
- Wir haben eine Richtlinie zu kryptografischen Kontrollen zum Schutz von Informationen. Dies ist besonders wichtig beim Austausch von Informationen mit Kunden mit einem hohen Informationssicherheitsprofil.
- Wir arbeiten mit einem Business Continuity-Plan, in dem die Informationssicherheit eine wichtige Rolle spielt. Details zur Organisation der Geschäftskontinuität finden Sie im BCP.
- Wir halten uns an das Gesetz in Bezug auf Datenschutz, geistiges Eigentum und Wettbewerb. Eine Übersicht über relevante Gesetze und Vorschriften ist in unserem integrierten Managementhandbuch enthalten.

Datenschutzrichtlinie

Unsere Datenschutzrichtlinie konzentriert sich auf die folgenden Aspekte:

- Wir sind transparent in unserer Kommunikation mit Kunden, Partnern und (Regierungs-) Behörden in Bezug auf Datenschutz.
- Wir haben einen Datenschutzbeauftragten / Datenschutzbeauftragten ernannt, um die Einhaltung der DSGVO und verwandter Gesetze und Vorschriften sicherzustellen.
- Wir stellen sicher, dass wir immer die gesetzlichen Anforderungen für die Datenverarbeitung erfüllen. Zu diesem Zweck gelten folgende Grundsätze:
 - Zweckbindung: Personenbezogene Daten werden nur für den im Verarbeitungsregister angegebenen Zweck verarbeitet.
 - Rechtmäßigkeit: Alle personenbezogenen Daten werden auf der Grundlage einer klaren rechtlichen Grundlage verarbeitet.
 - Minimale Datenverarbeitung: Unsere Organisation verarbeitet nur personenbezogene Daten, die für den jeweiligen Zweck erforderlich sind.
 - Richtigkeit der Verarbeitung und Datenlöschung: Personenbezogene Daten, die verarbeitet werden, sind korrekt und werden bei Bedarf aktualisiert. Darüber hinaus werden personenbezogene Daten, die keinen Zweck mehr erfüllen, aktiv gelöscht.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 33 von 36

- Speicherung personenbezogener Daten: Personenbezogene Daten werden so gespeichert, dass Personen nur für die Zwecke identifiziert werden können, für die die Daten verarbeitet werden. Werden personenbezogene Daten zu Archivzwecken im öffentlichen Interesse, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken für längere Zeiträume gespeichert, werden geeignete technische und organisatorische Maßnahmen ergriffen, um sicherzustellen, dass die Rechte und Freiheiten von Personen geschützt werden.
- Technische und organisatorische Maßnahmen: Unsere Organisation ergreift technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor unrechtmäßiger Verarbeitung, Verlust, Zerstörung oder Beschädigung. Bitte beachten Sie unsere Informationssicherheitsrichtlinie für weitere Details.

Unsere Organisation hat daraufhin die folgenden Maßnahmen ergriffen:

- Wir führen ein Verarbeitungsverzeichnis, das alle mit personenbezogenen Daten verbundenen Verarbeitungstätigkeiten sowohl im Hauptprozess als auch in unterstützenden Prozessen auflistet.
- Um die bedeutendsten Risiken zu identifizieren, führt unsere Organisation eine Datenschutz-Folgenabschätzung (DPIA) durch. Auf der Grundlage der identifizierten Risiken werden technische und organisatorische Maßnahmen ergriffen, um diese Risiken zu mindern.
- In Fällen, in denen unsere Organisation als Datenverantwortlicher handelt, werden mit Auftragsverarbeitern Datenverarbeitungsverträge abgeschlossen. Der Verarbeitungsvertrag beschreibt den Zweck, die Art, den Umfang, die Dauer und die technischen und organisatorischen Maßnahmen.
- Wir verwalten Datenverstöße nachweislich über einen etablierten Workflow. Abhängig von der Auswirkung des Datenverstosses werden Benachrichtigungen an die Aufsichtsbehörde und betroffene Personen versandt. Die Rechte, die betroffene Personen ausüben können, sind in der Datenschutzerklärung auf unserer Website beschrieben.
- Die Erklärung beschreibt auch den Prozess zur Einreichung von Anfragen. Unsere Organisation hat einen internen Prozess zur angemessenen Bearbeitung von Anfragen eingerichtet. Betroffene Personen können Zugang, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch gegen die Verarbeitung beantragen.
- Unsere Mitarbeiter sind sich der von ihnen verarbeiteten personenbezogenen Daten bewusst und handeln entsprechend. Der Verhaltenskodex für Datenschutz und Informationssicherheit ist das Leitprinzip. Unsere Organisation hat einen Datenschutzbeauftragten (DSB) ernannt. Der DSB stellt sicher, dass personenbezogene Daten gemäß den Anforderungen der DSGVO verarbeitet und geschützt werden. Der DSB arbeitet auch auf Anfrage mit der Aufsichtsbehörde zusammen und erfüllt gegebenenfalls die Rechte der betroffenen Personen. Eine vollständige Übersicht über die Verantwortlichkeiten und Befugnisse des DSB ist in der Stellenbeschreibung enthalten.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 34 von 36

- Wir wenden das Prinzip des Datenschutzes durch Technikgestaltung an, wenn wir Mechanismen zur Verarbeitung personenbezogener Daten entwerfen und entwickeln, und berücksichtigen dabei die Privatsphäre der betroffenen Personen so weit wie möglich. Darüber hinaus beschränken wir die Verarbeitung personenbezogener Daten auf das für unsere Ziele erforderliche Maß und auf eine rechtliche Grundlage.
- Datenschutz durch Voreinstellung wird auf alle Systeme angewendet, wobei spezifische Rechte für einen Mitarbeiter je nach seiner Rolle verwendet werden. Alle Standardeinstellungen werden so gewählt, dass die Privatsphäre maximiert wird.
- Bei der Gestaltung und Aufrechterhaltung von Richtlinien zum Schutz von PII werden geltende PII-Gesetze und -Vorschriften berücksichtigt.

Richtlinienpunkte für Informationssicherheit und Datenschutz wurden in einen praktischen Verhaltenskodex für unsere Mitarbeiter übersetzt.

Klassifikation	Copyright ©	Seite
Vertraulich	Safeguard B.V.	Seite 35 von 36