ecard

SVC

Information Security Policy der SVC

Wien am 01. September 2019

ecard SVC

Inhaltsverzeichnis

1 Vorwort zur Information Security Policy

Die vorliegende Information Security Policy stellt für die gesamte Sozialversicherungs-Chipkarten Betriebs- und Errichtungsgesellschaft m.b.H. (SVC) die geschlossene und strukturierte Dokumentation zur Etablierung und Umsetzung der Informationssicherheit dar. Die Information Security Policy wurde im Auftrag der Geschäftsführung erstellt und basiert auf der Norm ISO 27000ff.

Diese Information Security Policy beschreibt die sicherheitsrelevanten Anforderungen, welche für alle physikalischen Systeme und Teilsysteme, für deren einzelne Komponenten, für jede Art von Software, Daten und Informationen, für Strukturen und Prozesse, für die erforderliche Infrastruktur sowie für alle internen und externen Mitarbeiterinnen und Mitarbeiter sowie Funktionsträger (Aufsichtsrat, Gesellschafter-Vertreter) gelten.

Mit der Information Security Policy wird keine Ausarbeitung geschaffen, welche lediglich den Charakter einer Momentaufnahme hat und mit der Änderung von technischen Randbedingungen oder Beurteilungen schnell an Wert verliert. Vielmehr ist diese ein fortschreibungsfähiges, lebendes Dokument.

Die Fortschreibung dieser Leitlinie erfolgt in definierten Zyklen, da jedes Sicherheitskonzept dynamische Komponenten besitzt, deren Änderungen Auswirkungen auf die identifizierten Risiken und damit auch auf die zu ergreifenden Sicherheitsmaßnahmen haben.

2 Allgemeines Sicherheitsleitbild

Die Geschäftsführung hat die Aufgabe, gemeinsam mit allen Mitarbeiterinnen und Mitarbeitern sowie externen Partnern die Vermögenswerte der SVC und die ihr von Dritten anvertrauten schützenswerten Güter zu bewahren.

Zu den Vermögenswerten der SVC zählen die materiellen Werte, wie etwa das Inventar und die immateriellen Werte, wie etwa das „Know How“ der Mitarbeiterinnen und Mitarbeiter. Zu den schützenswerten Gütern, die der SVC von Dritten anvertraut sind, zählen die von uns im Rahmen unserer Dienstleistung ver- und erarbeiteten Informationen.

Die Gesamtheit aller Schutzmaßnahmen wird regelmäßig auf deren Aktualität und Wirksamkeit kontrolliert, in einem Sicherheitsbericht dargelegt und zumindest einmal im Kalenderjahr in einem Management-Review bewertet.

Zur Aufrechterhaltung der angestrebten Informationssicherheitsstandards wird das Informationssicherheits-Management System einem kontinuierlichen Verbesserungsprozess unterzogen. Dieser Prozess betrachtet zumindest jährlich die Umsetzung von Sicherheitsmaßnahmen, den Betrieb und die Kontrolle des Informationssicherheits-Management-Systems und prüft generell die Informationssicherheits-Vorgaben auf ihre Angemessenheit und Sinnhaftigkeit.

Die in Folge beschriebene Information Security Policy stellt somit eine verbindliche Grundlage unseres Handelns dar.

3 Sicherheitsziele und Anforderungen

Das von der SVC eingeführte Informations-Sicherheits-Management-System (ISMS) orientiert sich an den Auflagen und Anforderungen der ISO 27000ff.

Unser Know-how befähigt uns, für Bereiche der Gesundheitstelematik und des E-Government Systemlösungen anzubieten und zu betreiben. Wartung, Pflege, Weiterentwicklung und Betrieb der Systeme und Dienstleistungen erfordern die Definition angemessener Sicherheitsziele.

Diese ergeben sich aus den Qualitäts- und Sicherheitsanforderungen der SVC, des Hauptverbands der österreichischen Sozialversicherungsträger (HVB), der Sozialversicherungsträger, der Vertragspartner (das sind u.a. Ärzte) und Versicherten (SV-Anspruchsberechtigten, das sind im Allgemeinen die Patienten) sowie den verschiedenen gesetzlichen Anforderungen.

Die Sicherheitsziele stellen die oberste Ebene der Sicherheitsanforderungen an alle Systeme und Prozesse der SVC dar. Sie beinhalten sechs Grundwerte (oberste Regeln bzw. Schutzziele), die nachfolgend aufgeführt sind. Diese Grundwerte müssen

- von den Verantwortlichen der SVC gelebt und ständig auf ihre Umsetzung überprüft werden,
- von allen Partnern der SVC berücksichtigt werden.

Darauf basierend leiten sich die systemspezifischen Schutzziele ab. die in der SVC in folgender Reihung umsetzt werden: Integrität vor Vertraulichkeit vor Verfügbarkeit.

- Integrität:

  Das höchstrangige Schutzziel ist die Integrität der Informationen, Systeme und Prozesse. Gesundheitsdaten müssen zu jeder Zeit korrekt sein, um eine erfolgreiche Anwendung sicherzustellen.

  Das Verhindern nicht autorisierter Modifikation und Manipulation der zu übertragenden Daten ist vom Unternehmen sicherzustellen. Die regelwidrige Generierung und Veränderung von Informationen, welche unter anderem die Anspruchsbelege, Abstimmungsdaten oder Signaturdaten darstellen, wird sicher verhindert. Es ist jederzeit sichergestellt, dass Erzeugung, Veränderung und Löschung von sicherheitsrelevanten Informationen ausschließlich nach definierten Regeln erfolgen. Die zu implementierenden Sicherheitsmechanismen zur Bewahrung der Integrität müssen eine hohe Widerstandsfähigkeit besitzen.

- Vertraulichkeit:

Die SVC stellt sicher, dass die Vertraulichkeit der Informationen nicht zu Gunsten der Verfügbarkeit eingeschränkt wird.

Die Daten müssen den Datenschutz- und Datensicherheitsanforderungen genügen. Die SVC stellt jederzeit sicher, dass alle schutzbedürftigen Informationen und Daten nur Berechtigten zur Kenntnis gelangen und nur von diesen Personen bzw. Systemen verarbeitet werden dürfen. Die Anforderungen an die Vertraulichkeit der Daten über die Inanspruchnahme von Gesundheitsdienstleistungen sowie der signaturrelevanten Daten sind hoch.

- Verfügbarkeit:
  Es ist von der SVC sicherzustellen, dass Daten, wenn sie benötigt werden, den berechtigten Personen bzw. Systemen zur Verfügung stehen. Zur Verfügbarkeit zählt auch die Betriebssicherheit von EDV-Systemen und Programmen, ebenso wie der Schutz vor Datenverlust. Störungen und Kompromittieren einzelner Komponenten werden entweder in den Auswirkungen beschränkt oder sicher verhindert. Der Systembetrieb kann auch bei Störungen von Systembestandteilen (Hardware, Software und Prozesse), Ausfall von sicherheitstechnischen Einrichtungen und Verlust der Vertraulichkeit dezentraler sicherheitstechnischer Einrichtungen weitergeführt werden. Die zu implementierenden Sicherheitsmechanismen zur Aufrechterhaltung der Verfügbarkeit müssen eine hohe Widerstandsfähigkeit besitzen.

- Authentizität:
  Authentizität (auch Fälschungsschutz) bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit. Die SVC stellt sicher, dass durch den Nachweis der Authentizität die Unverfälschtheit und die Urheberschaft der Daten bzw. Informationen nachgewiesen werden kann.

- Nicht-Abstreitbarkeit
  Bei der Nicht-Abstreitbarkeit (der Urheberschaft bzw. Verbindlichkeit des Absenders) geht es darum, dass eine Kommunikation im Nachhinein vom Absender gegenüber Dritten nicht abgestritten werden kann (engl. *non repudiation*). Wichtig ist dieses Ziel insbesondere für Dienstleister. Falls Verträge online abgeschlossen werden, ist die Nicht-Abstreitbarkeit sehr wichtig.

- Beweissicherung:
  Die SVC stellt sicher, dass die einzelnen Systeme und sicherheitsrelevanten Prozesse revisionsfähig sind. Die zu implementierenden Sicherheitsmechanismen zur Gewährleistung der Revisionsfähigkeit müssen **eine** mittlere Mechanismenstärke besitzen.

Diese Grundwerte (Sicherheitsziele) sowie alle mitgeltenden Unterlagen und Prozesse gelten für die gesamte SVC und sind für alle Mitarbeiterinnen und Mitarbeiter der SVC verbindlich.

3.1 Identifizierung und Authentisierung

3.1.1 zwischen Teilen der Systeme

Sicherheitstechnische Einrichtungen müssen sich gegenseitig bei jeder Transaktion eindeutig identifizieren und authentisieren. Die Authentizität der sicherheitstechnischen Einrichtungen muss während der gesamten Transaktion gewährleistet sein.

3.1.2 gegenüber Benutzer

Das jeweilige System muss je nach Kritikalität den Zugreifenden eindeutig identifizieren und authentifizieren. Dabei ist zu beachten, dass die Identifikation und Authentisierung vor dem ersten Zugriff zu erfolgen hat. Zusätzlich ist der Zeitraum, in dem weitere Zugriffe ohne erneute Identifikation möglich sind, zu beschränken.

3.2 Zugriffskontrolle

Änderungen von Außerhalb (z.B. Änderung der Anspruchsdaten) müssen über eine gesicherte Schnittstelle in das System übernommen werden. Änderungen anderer sicherheitsrelevanter Informationen dürfen nur durch dazu berechtigte sicherheitstechnische Einrichtungen bzw. auf Anforderung eines berechtigten Benutzers erfolgen.

Der schreibende bzw. modifizierende Zugriff auf sicherheitsrelevante Informationen darf nur identifizierten und authentisierten Teilen im System mittels festgelegter Prozesse nach einer Rechte-Prüfung möglich sein.

Der Zugriff auf Schlüsselwerte darf nur der hochsicherheitstechnischen Einrichtung, in der die hochsicherheitsrelevante Information gespeichert ist, möglich sein.

Der lesende Zugriff auf sonstige Protokollinformationen darf nur identifizierten und autorisierten Benutzern möglich sein.

Der erfolglose Versuch einer Identifikation oder Autorisierung darf keine für Angriffe verwertbaren Informationen über Identifikation- oder Autorisierung bzw. die dahinterstehenden Personen oder Einrichtung erbringen.

3.3 Beweissicherung

Für jeden aktiven sicherheitskritischen Teil eines Systems, mit Ausnahme der Chipkarten, muss eine Protokollierungskomponente vorhanden sein, die jede versuchte oder durchgeführte Generierung, Änderung oder Löschung von sicherheitsrelevanten Informationen protokolliert. Der Umfang der protokollierten Daten muss den Zwecken der Aufklärung von Zweifelsfällen in angemessener Zeit nach einer Interaktion und Behebung von Störungen genügen.

Die Systeme müssen Mechanismen enthalten, welche Ausfälle bzw. Störungen von Teilen des Systems und Übertragungskanälen erkennen und protokollieren. Änderung und vorzeitige Löschung von Protokollinformation muss zuverlässig verhindert werden.

Zentrale Komponenten müssen eine Protokollierungskomponente enthalten, die alle sicherheitsrelevanten Aktionen von Systembetreuern und Wartungstechnikern aufzeichnet.

Bei allen Protokollen ist mit geeigneten Methoden die Authentizität sicherzustellen.

3.4 Protokollauswertung

Werkzeuge zur Auswertung und Verwaltung von Protokolldaten müssen vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer oder Teile des Systems zu identifizieren.

Es muss einen Mechanismus zur Überwachung von Ereignissen geben, die entweder besonders sicherheitsrelevant sind oder aufgrund der Häufigkeit ihres Auftretens zu einer kritischen Bedrohung der Sicherheit des Systems führen könnten.

3.5 Wiederaufbereitung

Alle Speicherobjekte mit entsprechendem Schutzbedarf, die den Systemen wieder zur Verfügung gestellt werden, müssen vor einer Wiederverwendung durch andere Benutzer oder Prozesse so aufbereitet werden, dass keine Rückschlüsse auf ihren früheren Inhalt möglich sind.

3.6 Unverfälschtheit

Das Regelsystem zur Generierung, Veränderung und Löschung von sicherheitsrelevanten Informationen ist explizit zu formulieren und auf Sinnhaftigkeit und Widerspruchsfreiheit zu prüfen.

Für Entwicklung, Produktion, Test und nachträgliche Veränderung von sicherheitstechnischen Einrichtungen sind explizite Regeln zur Sicherstellung der Einhaltung der Sicherheitsziele zu formulieren und deren Einhaltung zu verifizieren.

Es sind Mechanismen zu implementieren, welche die Integrität jeder sicherheitsrelevanten Information und jeder sicherheitstechnischen Einrichtung vor ihrer Verwendung verifizieren. Die Konfiguration jeder sicherheitstechnischen Einrichtung muss identifizierbar, überprüfbar und gesichert sein.

3.7 Zuverlässigkeit der Dienstleistung

Es müssen Mechanismen vorhanden sein, die im Fall des Verlustes der Vertraulichkeit von dezentralen Komponenten eine sichere Fortführung des Betriebes innerhalb einer festgelegten Zeit ermöglichen. Zentrale Komponenten sind physisch zu sichern.

Es müssen geeignete technische und organisatorische Maßnahmen vorgesehen sein, um Ausfälle und Teilausfälle von Komponenten des jeweiligen Systems so zu überbrücken, dass alle fortlaufend benötigten Funktionen auch im Rest-System zur Verfügung stehen.

Nach der Behebung eines solchen Ausfalls muss die Komponente wieder so in das System integriert werden können, dass ein kontinuierlicher Betrieb der fortlaufend benötigten Funktionen auch im Rest-System gewährleistet ist. Sobald ausgefallene Online-Komponenten wieder verfügbar werden, wiederholen die vom Ausfall betroffenen sicherheitstechnischen Einrichtungen die als fehlerhaft protokollierten Nachrichten und Prozesse, bis der Zustand wiederhergestellt ist, den das System ohne Ausfall eingenommen hätte.

Kann dieser Zustand innerhalb einer vorgegebenen Zeit nicht wiederhergestellt werden, meldet das System einen gravierenden Systemfehler.
Werden Komponenten auch für andere Anwendungen genützt, ist zuverlässig sicherzustellen, dass dadurch keine Beeinträchtigung der Sicherheit eintritt.

3.8 Übertragungssicherung

3.8.1 Datenvertraulichkeit

Die Systeme müssen sicherheitsrelevante Informationen zwischen den sicherheitstechnischen Einrichtungen mittels eines hinreichend sicheren Algorithmus verschlüsselt übertragen.

3.8.2 Datenintegrität

Die Systeme müssen so entworfen sein, dass Übertragungsfehler und Verletzungen der Integrität sicher als solche erkannt und korrigiert werden können.

Die Kommunikationsprotokolle zu anderen sicherheitstechnischen Einrichtungen/technischen Einrichtungen enthalten Mechanismen, die Verletzungen der Integrität im System durch zufällige oder beabsichtigte Beeinflussung am Kommunikationsweg sicher erkennen lassen oder verhindern.

Es muss ein Mechanismus existieren, der im Fall der Verletzung der Integrität den ursprünglichen Zustand der Daten wiederherstellt und die Wiederholung des Datenaustausches ermöglicht.

Das System muss Mechanismen hoher Wirksamkeit enthalten, die unbefugte Manipulationen von sicherheitsrelevanten Informationen erkennen lassen. Die Manipulation von Protokolldaten soll mit mittlerer Wirksamkeit erkannt werden können.

Das System muss Mechanismen hoher Wirksamkeit enthalten, die das Wiedereinspielen von Daten erkennen lassen.

3.8.3 Sende- und Empfangsnachweise

Übertragene Informationen werden so gekennzeichnet, dass der Empfänger den Absender eindeutig verifizieren kann.

Es ist ein Mechanismus einzusetzen, der es dem Absender von Informationen ermöglicht, den Empfang durch einen eindeutig identifizierten und authentisierten Empfänger festzustellen.

3.9 Wissensteilung

Informationen über die Systeme und Produktionsmittel sind so zwischen Organisationseinheiten aufzuteilen, dass keine Organisationseinheit allein in der Lage ist, sicherheitstechnische Einrichtungen oder sicherheitsrelevante Informationen zu erzeugen oder zu verfälschen. Die Mitglieder der Organisationseinheit sind über Sinn und Wirkung und Handhabung der Wissensteilung nachweislich zu belehren.

3.10 Nachweis der Wirksamkeit / Revision

Die Wirksamkeit der obligatorischen Mechanismen ist vom Unternehmen in regelabhängigen Zeitabständen nachzuweisen.

3.11 Kryptografisches Konzept

Sofern die Sicherung der Integrität, Verfügbarkeit oder Beweissicherung auf ein kryptografisches Konzept aufbaut, wird ein solches explizit definiert und auf Konsistenz mit der Information Security Policy geprüft.

Die Vertraulichkeit bei der elektronischen Weitergabe von Gesundheitsdaten wird dadurch sichergestellt, dass die elektronische Weitergabe von Gesundheitsdaten in der SVC nur über Netzwerke durchgeführt wird, die entsprechend dem Stand der Technik in der Netzwerksicherheit gegenüber unbefugten Zugriffen abgesichert sind.

Die Absicherung des Datenverkehrs:

- erfolgt durch kryptographische oder bauliche Maßnahmen.
- Der Netzzugang ist ausschließlich für eine geschlossene oder abgrenzbare Benutzerinnen- bzw. Benutzergruppe vorgesehen.
- Es erfolgt eine Authentifizierung der Benutzerinnen und Benutzer.

Oder, dass Protokolle und Verfahren verwendet werden,

- die die vollständige Verschlüsselung der Gesundheitsdaten bewirken und
- deren kryptographische Algorithmen in der GTelV 2013 angeführt sind.

Die Auswahl eines kryptografischen Verfahrens zerfällt in die beiden Teilaufgaben

- Auswahl des kryptografischen Algorithmus und
- Auswahl einer technischen Realisierung.

Auswahl von kryptografischen Algorithmen
Bei der Auswahl von kryptografischen Algorithmen wird zunächst geklärt, welche Art kryptografischer Verfahren benötigt werden: also symmetrische, asymmetrische oder hybride Verfahren. Dann werden geeignete Algorithmen, also solche mit entsprechender Mechanismenstärke, ausgewählt.

Realisierbarkeit von technischen Anforderungen
Die Chiffrieralgorithmen müssen so beschaffen sein, dass die technischen Anforderungen, insbesondere die geforderte Performance, durch eine geeignete Implementation erfüllt werden können. Aber auch Anforderungen an Synchronisationsoverhead und Zeitverzögerung (z.B. falls "Echtzeit"-Verschlüsselung von großen Datenmengen erfordert wird). Mit dieser Vorgehensweise sichert die SVC eine Bewertung der Sicherheit ausgewählter kryptografischer Verfahren und ermöglicht damit eine längerfristige Orientierung bei der Wahl jeweils geeigneter Methoden.

3.12 Rechtssicherheit

Die SVC stellt sicher, dass unbefugte Manipulationen strafrechtlich verfolgt werden können.

4 Risikomanagement

Ziel des Informationssicherheits-Risikomanagements ist, dass die SVC ihre wichtigsten Risiken

- finden und erkennen
- bewerten
- bewältigen
- überwachen

kann.

Die SVC legt Informationssicherheitsqualitätsziele fest und orientiert sich dabei am Bewertungssystem der Ratings nach der Standard & Poors Ratingklassifikation:

- Der Schutz aller wesentlichen, unternehmensrelevanten Ressourcen und Prozesse ist entsprechend dem aktuellen Stand der Technik abgesichert. Dieser wird laufend überprüft, aktualisiert und erforderliche Schutzmaßnahmen werden angepasst.
- IT-Risk Management ist Bestandteil der Unternehmensstrategie.
- Die SVC verfolgt im Informationssicherheits-Risikomanagement die Systematik der ISO 31000 und das „Plan-Do-Check-Act“- Modell.

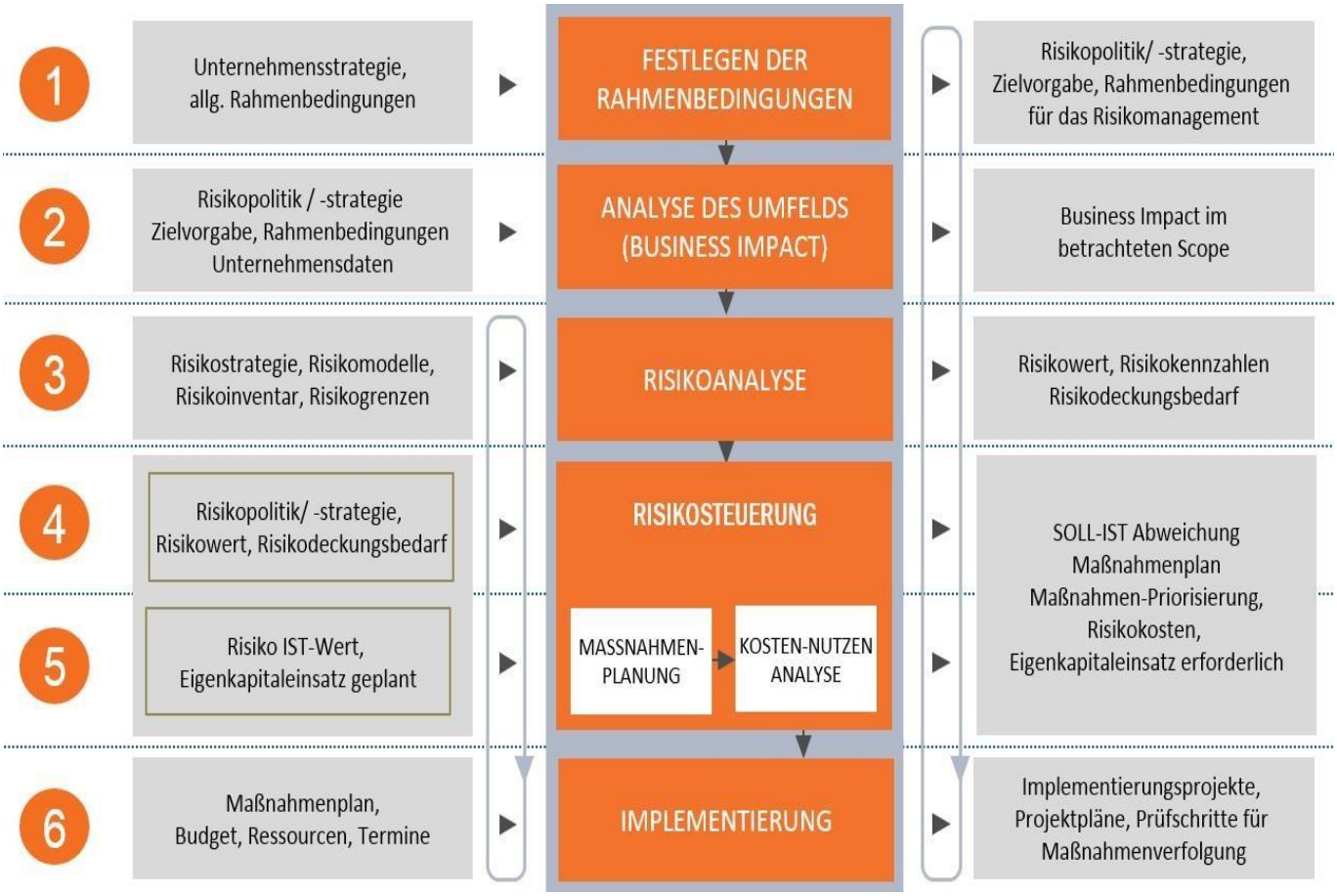

Abbildung 1: Prozess Informationssicherheit-Risikomanagement

5 Verantwortlichkeiten

5.1 Geschäftsführung

Die Gesamtverantwortung für Informationssicherheit in der SVC liegt bei der Geschäftsführung. Die Geschäftsführung ist insbesondere verantwortlich für (siehe dazu auch ISO 27000ff)

- die Überprüfung und die Abnahme der Information Security Policy,
- das Vertreten der Information Security Policy nach innen und außen,
- die Informationssicherheits-Organisation sowie
- die strategische Ausrichtung der Informationssicherheit.

Diese Verantwortung ist nicht delegierbar. Die Geschäftsführung bedient sich jedoch in der Umsetzung des Informationssicherheits-Management-Teams.

5.2 Chief Information Security Officer (CISO)

Der Chief Information Security Officer (CISO) der SVC bildet das zentrale und unternehmensweite Steuerungsorgan für Informationssicherheit.

Der CISO ist im Besonderen verantwortlich für die

- Planung und Durchführung des Informationssicherheits-Risikomanagementprozesses
- Erstellung von Sicherheitsrichtlinien
- Planung und Umsetzung der Sicherheitsmaßnahmen

und berichtet direkt an die Geschäftsführung über sicherheitsrelevante Themen und Projektanträge.

5.3 Informationssicherheits-Management-Team

Das Informationssicherheits-Management-Team (SMMT) besteht aus der Geschäftsführung, dem Vertreter für rechtliche Angelegenheiten, den Bereichsleiterinnen und Bereichsleitern, dem Datenschutzbeauftragten und dem Chief Information Security Officer.

5.4 Mitarbeiterinnen und Mitarbeiter

Die Mitarbeiterinnen und Mitarbeiter, die Führungskräfte und die Informationssicherheits-Organisation sind die Basis für eine angemessene Informationssicherheit im Unternehmen. Erreicht wird das geforderte Maß an Informationssicherheit dadurch, dass alle Mitarbeiterinnen und Mitarbeiter für die vorliegende Information Security Policy sensibilisiert sind, die daraus

abgeleiteten Sicherheitsrichtlinien und Sicherheitsmaßnahmen beachten und die jeweiligen Tätigkeiten danach ausrichten.

5.5 Externe Partner

Die Bedeutung der Informationssicherheit für die SVC wird externen Partnern verdeutlicht. Sie sind verpflichtet, bei der Erbringung ihrer Dienstleistung für die SVC die vorliegende Information Security Policy und die auf die zu erbringende Dienstleistung zutreffenden gültigen Sicherheitsstandards und -richtlinien einzuhalten.

Wenn notwendig, ist mit dem externen Partner ein Geheimhaltungsvertrag, (auch Geheimhaltungserklärung, Geheimhaltungsvereinbarung, Vertraulichkeitsvereinbarung, Verschwiegenheitsvereinbarung, NDA (Abkürzung für Englisch non-disclosure agreement) oder CDA (Abkürzung für Englisch confidential disclosure agreement)) abzuschließen, welcher regelt, wie der externe Partner mit ihm zugänglich gemachten Informationen umzugehen hat.

6 Umsetzung

Die Umsetzung des ISMS der SVC erfolgt durch hierarchisch erstellte Sicherheitsrichtlinien und Sicherheitsmaßnahmen (siehe Abb.1), welche nach ISO 27000ff erstellt werden.

6.1 Informationssicherheits-Architektur

In der Informationssicherheits-Architektur wird festgelegt, wie die Informationssicherheit in der SVC umgesetzt wird.

Abbildung 2: Informationssicherheits-Architektur der SVC

Auf der obersten Ebene der Informationssicherheits-Architektur findet sich die Information Security Policy, welche die Sicherheitsziele und Verantwortlichkeiten festlegt und unternehmensweit Gültigkeit hat. Die Information Security Policy bildet den Rahmen für die Sicherheitsrichtlinien und Sicherheitsmaßnahmen. Die Sicherheitsrichtlinien beschreiben die grundlegenden Sicherheitsanforderungen auf Basis der definierten Information Security Policy. Diese Sicherheitsrichtlinien werden, sofern dies notwendig ist, durch spezielle Sicherheitsmaßnahmen spezifiziert, die im Detail technische bzw. organisatorische Durchführungsbestimmungen enthalten. Sicherheitsmaßnahmen können auf Unternehmensebene festgelegt, aber auch in einzelnen Bereichen oder Projekten nach den jeweiligen Anforderungen definiert werden.

6.2 Geltungsbereich

Zum direkten Geltungsbereich der Information Security Policy zählen alle Bereiche im direkten Einfluss der SVC. Zusätzlich zu diesem Bereich gehören noch all jene Objekte, welche zwar nicht im Einflussbereich der SVC stehen, aber einen essentiellen Einfluss für die Erfüllung der

Kernaufgaben der SVC haben (indirekter Geltungsbereich). Für all jene Objekte, welche zwar nicht im Einflussbereich der SVC sind, aber im physikalischen oder logischen Bereich der SVC stehen (z.B. Fremd-Netzwerk-Anschluss), gilt als Grenze des Geltungsbereichs der jeweilige Übergabepunkt. Informationssicherheit ist im gesamten - im direkten und indirekten - Geltungsbereich der SVC zu berücksichtigen.

6.3 Kontrolle

Der Umgang mit sicherheitsrelevanten Ressourcen wird so gestaltet, dass Verstöße gegen die Sicherheitsziele und ihre Verursacher feststellbar und zuordenbar sind (Grundsatz der Nachvollziehbarkeit und Revisionsfähigkeit). Dabei ist von der SVC sicherzustellen, dass diese Maßnahmen der Informationssicherheit im Einklang mit gesetzlichen und arbeitsrechtlichen Vorschriften erfolgen und ein Missbrauch dieser Maßnahmen für andere Zwecke, insbesondere solche, welche die Menschenwürde verletzen, ausgeschlossen wird.

Verstöße gegen die Informationssicherheitsziele sind insbesondere:

- die unautorisierte Preisgabe von Geschäfts- und Betriebsgeheimnissen,
- die Abfrage von Daten für nicht dienstliche Zwecke,
- die ungesicherte Verwahrung von Daten,
- die unautorisierte Weitergabe von Daten,
- die Verfälschung von Daten,
- die unautorisierte Veränderung sicherheitsrelevanter Ressourcen,
- die tatsächliche oder potenzielle finanzielle Schädigung der SVC durch Nichterfüllung von Sicherheitsmaßnahmen und
- die tatsächliche oder potenzielle Beeinträchtigung/Schädigung der Sicherheit von Patienten, Sozialversicherungsträgern und Vertragspartnern durch Nichterfüllung von Sicherheitsmaßnahmen.

7 Gesetzliche und normative Rahmenbedingungen

Folgende Gesetze und Verordnungen in der jeweils geltenden Fassung beeinflussen die Information Security Policy:

Allgemeines Sozialversicherungsgesetz ASVG § 31a bis c, §460/5, §460a	Aufgabenbereiche der SVC iZm ELSY Verschwiegenheitspflicht für Bedienstete
Allgemeines Sozialversicherungsgesetz (ASVG). § 31d Aufgaben des HVSV iZm ELGA	Beschreibung der Aufgaben als Auftrags-verarbeiter des Hauptverbandes
Arbeitnehmerschutzgesetze	Schutz der Arbeitnehmer, insb. ArbeitnehmerInnenschutzgesetz (ASchG), Arbeitszeitgesetz (AZG), Arbeitsruhegesetz (ARG)
Arbeitsverfassungsgesetz (ArbVG)	Einschaurechte / Mitwirkungsrechte des Betriebsrates
Bundesabgabenordnung (BAO)	Angelegenheiten der öffentlichen Abgaben
Bundesvergabegesetz 2018	Vertrauliche Behandlung von Bieter-Informationen
Datenschutz - Grundverordnung (DSGVO)	Schutz von personenbezogenen Daten (anwendbar ab 25.05.2018) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
Datenschutzgesetz (DSG) Durchführungsbestimmungen	(anwendbar ab 25.05.2018)
E-Commerce-Gesetz (ECG)	Elektronische Geschäftsabwicklung
EDV Handbuch der Österreichischen Sozialversicherung, Modul Technische Architektur und Standards (TAS)	Diverse Sicherheitsrichtlinien
E-Government-Gesetz (E-GovG)	Kundenservices über das Internet, Umsetzung der Amtssignatur

eIDAS-Verordnung (eIDAS-VO)	Verwendung elektronischer Signaturen und Vertrauensdienste Verordnung (EU) Nr. 910/2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. Nr. L 257/73 vom 28. August 2014
ELGA-Verordnung 2015: insbesondere Regelungen für ELGA-Komponenten und e-Medikation	Beschreibung der Aufgaben als Auftragsverarbeiter des Hauptverbandes
Gesundheitstelematikgesetz 2012 (GTelG 2012)	Datensicherheitsmaßnahmen bei der elektronischen Übermittlung von Gesundheitsdaten (einschließlich die Elektronische Gesundheitsakte)
Gesundheitstelematikverordnung 2013 (GTelV 2013)	Durchführungsbestimmungen zum Gesundheitstelematik-Gesetz
GmbH-Gesetz (GmbHG)	Allgemeine Rechtsvorschrift
Grundschutz BSI	Empfehlungen des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI), Quelle: www.bsi.bund.de
Informationssicherheitsgesetz (InfoSiG)	Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen
ISO 27000ff	Normenreihe für Informationssicherheits-Managementsysteme, Quelle: Austrian Standards Institute (ASI) vormals ÖNORM
Österreichisches Informationssicherheitshandbuch	Beschreibung und Unterstützung der Vorgehensweise zur Etablierung eines umfassenden Informationssicherheits-managementsystems in Unternehmen und der öffentlichen Verwaltung (Bundeskanzleramt in Kooperation mit A-SIT), Quelle: www.sicherheitshandbuch.gv.at

Richtlinien über die Zusammenarbeit der Sozialversicherungsträger und des Hauptverbandes in der elektronischen Datenverarbeitung 2006 (REDV 2006)	Aufgaben und Pflichten der SVC als IT-Tochter des HVB
Sicherheitsrichtlinie für die gesetzliche Sozialversicherung (SV-Sicherheits-richtlinie 2019 – SV-SR 2019)	Beschreibung von einheitliche Vorgangsweisen bei Sicherheitsthemen für alle SV-Organisationen und SV-Unternehmen
Signatur- und Vertrauensdienste-verordnung (SVV) (SigV)	Durchführungsbestimmungen zum Signatur- und Vertrauensdienstegesetz
Signatur- und Vertrauensdienstegesetz (SVG)	Verwendung elektronischer Signaturen und Vertrauensdienste–Durchführungsbestimmungen zur eIDAS-Verordnung
Strafgesetzbuch §§ 118-124, § 126a, § 148a	Strafbestimmungen für Verletzung der Verschwiegenheit, Computerkriminalität und Datenmissbrauch
SV-Datenschutzverordnung 2018 (SV-DSV 2018)	Basis für die SVC Datenschutz– und Datensicherheitsvorschrift
Telekommunikationsgesetz 2003 (TKG 2003)	Förderung des Wettbewerbes im Bereich der elektronischen Kommunikation
Unternehmensgesetzbuch (UGB)	Allgemeine Rechtsvorschrift
Urheberrechtsgesetz	Schutz von geistigem Eigentum, Software-Lizenzen
Verbandsverantwortlichkeitsgesetz (VbVG)	Verpflichtet zu klaren Regelungen, auch im Bereich Datenschutz
Zustellgesetz (ZustG)	Zustellung behördlicher Dokumente

8 Gültigkeitsbereich

Dieses SVC Security Dokument in dieser Version ist ab dem 01.09.2019 verbindlich und integraler Bestandteil der Allgemeinen Geschäftsbedingungen.

Dieses Dokument ist in der jeweils aktuellen Version auf der Website www.svc.co.at für alle interessierten Parteien verfügbar.

Dieses Dokument ist in der jeweils aktuellen Version Bestandteil jeder Einladung zur Angebotslegung.

Zusätzlich werden folgende Dokumente außer Kraft gesetzt:

- Alle früheren Versionen