DIE POST

Einfach sicher

IncaMail

Informationssicherheit

Version: V01.15

Datum: Mai 2022

Inhaltsverzeichnis

1 Einleitung

Mit IncaMail stellt die Post CH Kommunikation AG eine Plattform für den vertraulichen und nachweisbaren E-Mail Austausch zur Verfügung. Dabei stützen wir uns technisch wie rechtlich auf Standards und ermöglichen es, integriert in bestehende Prozesse, Informationen (E-Mail) zwischen Anwendern und Systemen vertraulich und nachweisbar auszutauschen. Dazu bieten wir verschiedene Identifikations- und Sicherheitsstufen, welche sich am Geschäftsfall / Anwendungsfall orientieren.
Je nach Geschäftsfall / Anwendungsfall sind unterschiedliche Anbindungsarten vorgesehen, Mail Gateway Integration (MGI), Enterprise Application Integration (EAI) oder Web-Interface (WI).

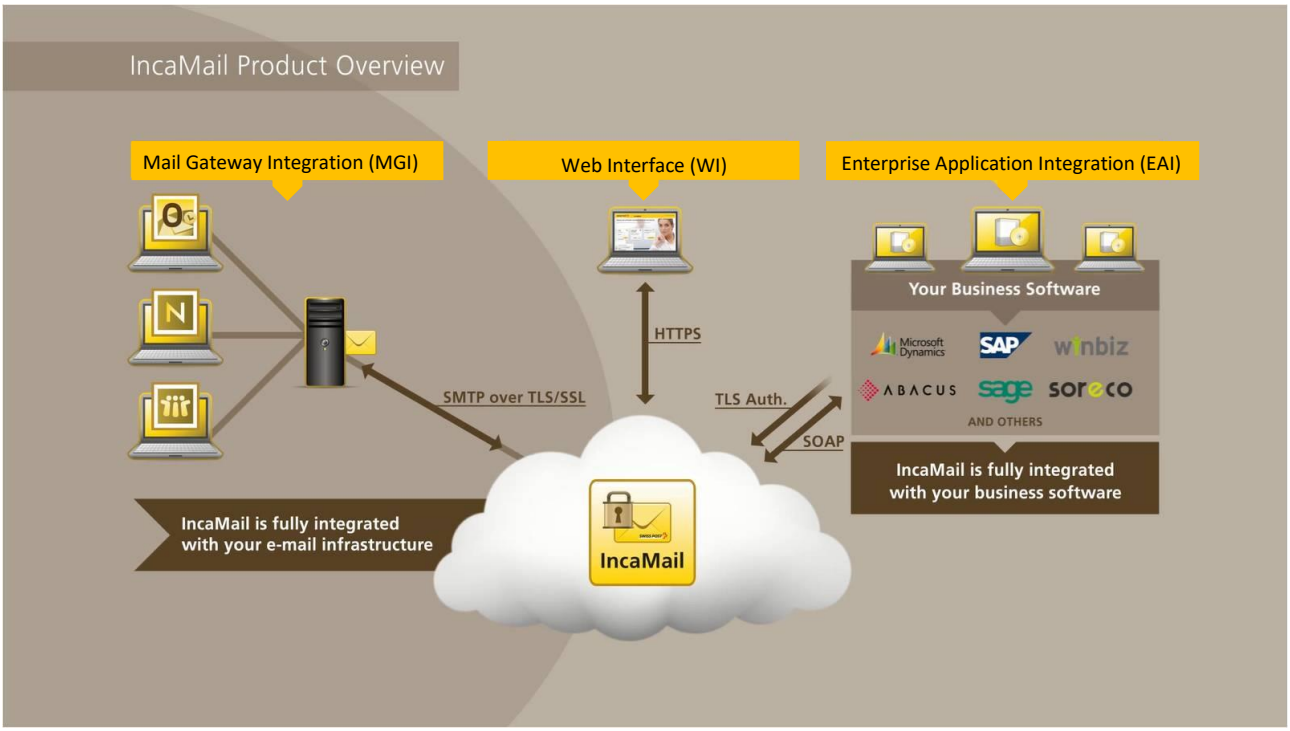
2 Grundsätze

Die Post CH Kommunikation AG hält mit IncaMail zur Sicherstellung der Informationssicherheit die folgenden Grundsätze ein, woraus sich auch das Akronym INCA ergibt:

- **I**ntegrity
- **N**on-repudiability
- **C**onfidentiality
- **A**uthentication

Integrity (Integrität):	Die Nachrichten bleiben unverändert. Die Post CH Kommunikation AG stellt sicher, dass Daten während des Transports nicht verändert werden.
Non-repudiability (Nicht-Abstreitbarkeit):	Versand und Empfang sind nachweisbar. Die Abholung der Nachrichten wird bei IncaMail dokumentiert. Bei Einschreiben erhält der Sender einen Nachweis als digital signierte Quittung mit Zeitstempel.
Confidentiality (Vertraulichkeit):	Die Daten können von Dritten nicht eingesehen werden. IncaMail überträgt sämtliche Daten mittels verschlüsselter Verbindung.
Authentication (Authentifikation):	Die Benutzer sind durch die Angabe ihrer E-Mail-Adresse und falls erforderlich mit der physischen Adresse bei der erstmaligen persönlichen Registrierung und durch die Eingabe der entsprechenden Aktivierungscodes identifiziert. Handelt es sich nicht um eine persönliche IncaMail-Nutzung, sondern um eine Unternehmensdomänen-Anbindung, erfolgt die Authentifikation über einen schriftlichen IncaMail Service Vertrag.

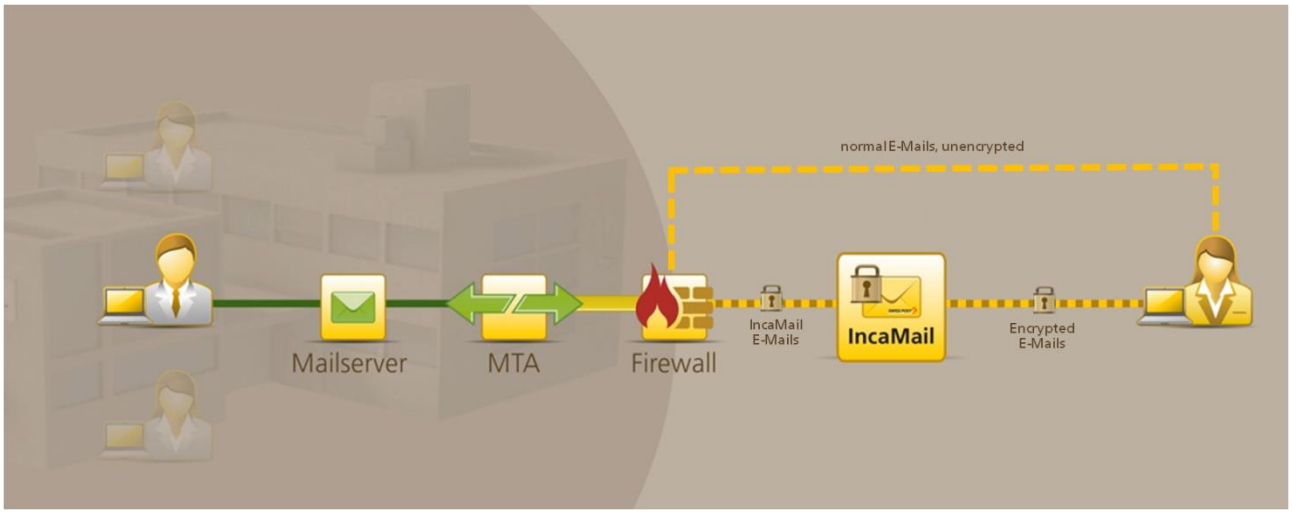
3 Anbindungsarten



IncaMail bietet unterschiedliche Anbindungsarten, welche je nach Kundenbedürfnis zum Einsatz kommen. In den folgenden Kapiteln ist jede Anbindungsart kurz erklärt.

3.1 Mail Gateway Integration (MGI)

Der Kunde verbindet seinen Mail Gateway zum Versand und Empfang von Nachrichten mit einer verschlüsselten Leitung mit IncaMail.
Die Gateway-Funktion wird im eigenen Firmennetz des Kunden aufgeschaltet. Der bestehende Mail Gateway des Kunden wird durch den Kunden so konfiguriert, dass normale E-Mails weiterhin über die eigene Infrastruktur versendet und empfangen und nur IncaMail-Nachrichten über eine verschlüsselte Verbindung an die Plattform IncaMail übergeben werden.

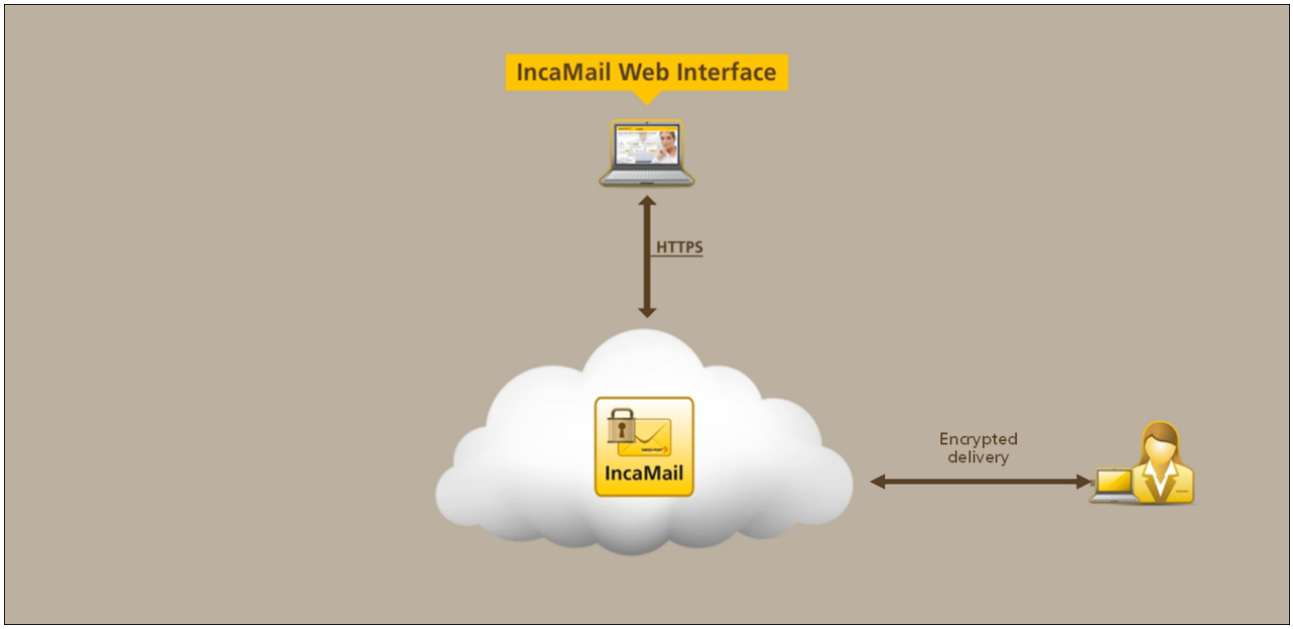


Eingehende Nachrichten werden über eine gesicherte und verschlüsselte Verbindung dem Mail Gateway des Kunden übergeben. Bei eingehenden Nachrichten ab dem Gateway des Kunden und bei abgehenden Nachrichten bis zur

Übergabe an die IncaMail-Plattform ist der Kunde für die Integrität und Vertraulichkeit der Nachrichten im eigenen Netzwerk selbst verantwortlich.
IncaMail nimmt nur Nachrichten vom Mail Gateway des Kunden entgegen, die mittels TLS-Verschlüsselung (inkl. Zertifikatsauthentisierung) übermittelt werden und liefert Nachrichten nur an den Mail Gateway des Kunden aus, wenn eine TLS-Verschlüsselung (inkl. Zertifikatsauthentisierung) aufgebaut werden kann (Enforcement). Die technische Anbindung der IncaMail-Kunden findet also verschlüsselt statt, wobei sich die Verschlüsselungstechnik am Stand der Technik orientiert.

3.2 Web Interface (WI)

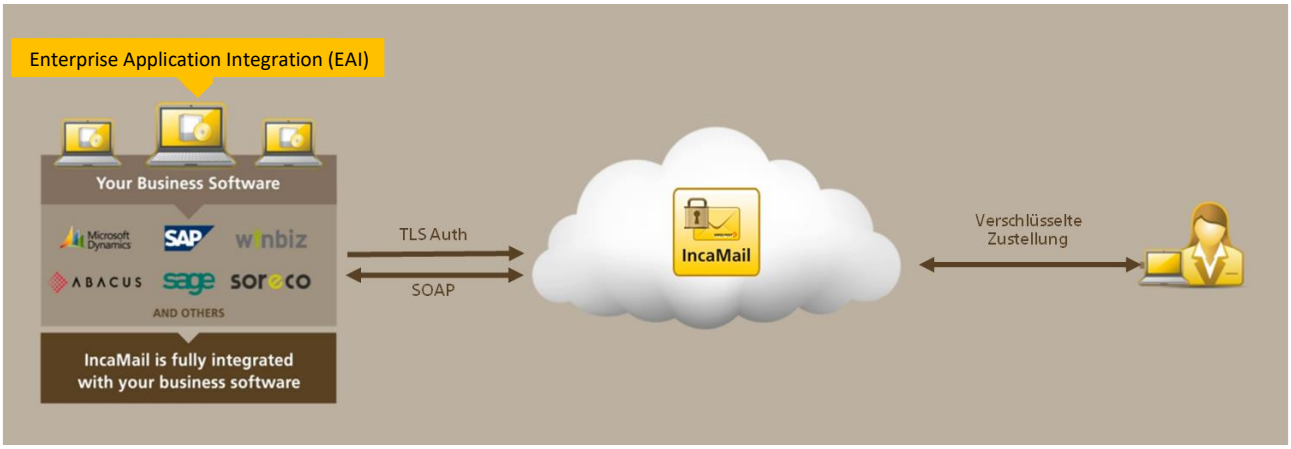
Mittels IncaMail Web Interface können Sie IncaMail direkt aus Ihrem Webbrowser nutzen und erhalten diese verschlüsselten E-Mails direkt in Ihrem gewohnten Posteingang.



IncaMail kann direkt via Web-Interface zum Senden und Empfangen von E-Mails benutzt werden – unabhängig von Ihrem Standort und benutztem Endgerät (PC oder mobile Geräte).

3.3 Enterprise Application Integration (EAI)

Mittels EAI kann der Versand und Empfang direkt in die Business Software integriert werden.



Dazu bietet IncaMail die beiden Schnittstellen SOAP Webservice (HTTPS) und TLS Auth (SMTP over TLS) an. Dabei findet die Authentifizierung mittels gültigem Benutzernamen/Passwort statt.
Die Schnittstelle TLS Auth kann einzig für den Versand von Nachrichten genutzt werden.
Mittels SOAP Webservice können sowohl Nachrichten gesendet wie auch empfangen werden. Im Fall des Empfangens können verschlüsselte Attachments mittels „SOAP decrypt“ entschlüsselt werden.

4 Versand grosser Dateien (Large File Transfer (LFT))

Für Kunden, die IncaMail in ihre Mailinfrastruktur integriert haben (Mailgateway Integration, MGI) bietet IncaMail die Möglichkeit, grosse Datenmengen via Large File Transfer zu versenden. Mithilfe des IncaMail-Add-ins können Datenmengen von bis zu 1 GB sicher via IncaMail versandt werden. Für die Nutzung des Large File Transfer fallen keine zusätzlichen Kosten an.

Via Drag-and-drop oder Klick in die entsprechende Zone laden Sie die gewünschten Dateien über eine gesicherte Verbindung auf den IncaMail-Server. Die Daten bleiben dabei ausschliesslich verschlüsselt auf dem IncaMail-Server der Schweizerischen Post gespeichert. Beachten Sie, dass die Dateien auf dem IncaMail-Server während maximal sieben Tagen zum Download zur Verfügung stehen und anschliessend unwiderruflich gelöscht werden. Nach erfolgreichem Upload werden direkt in der aktuellen Nachricht Links generiert, über die der Empfänger die Dateien herunterladen kann. Versenden Sie das E-Mail wie gewohnt geschützt via IncaMail an die gewünschten Empfänger. Da die Dateien nicht direkt dem E-Mail angehängt werden, wird die Grösse des E-Mails nur geringfügig beeinflusst.

Der Large File Transfer (LFT) von IncaMail kann auch im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV, SR 172.021.2), in Zivil- und Strafprozessen und in Schuldbetreibungs- und Konkursverfahren (VeÜ-ZSSV, SR 272.1) genutzt werden (siehe IncaMail für Behörden). IncaMail ist eine vom Bund anerkannte sichere Zustellplattform.

5 Verarbeitung

IncaMail ist eine Plattform für den nachvollziehbaren und vertraulichen Austausch von E-Mails. Um sowohl die unterschiedlichen Anbindungsarten als auch die Prüfung auf Schadsoftware zu unterstützen, befinden sich Inhaltsdaten im Rahmen des Versand-, Abholungs- und Leseprozesses für maximal 90 Tage auf der Plattform. Selbstverständlich werden diese nach Abschluss dieser Zeit umgehend gelöscht. Auch sorgen die ISO 27001 zertifizierten Prozesse dafür, dass während dieser Versand-, Abholungs- und Leseprozesse kein Unberechtigter (z.B. Administrator) Zugriff hat.

6 Leistungsumfang IncaMail nach Versandarten

Leistung	Vertraulich	Persönlich	Einschreiben
Identifikation Absender	Mind. Verifikation E-Mail-Adresse oder Geschäftskundenvertrag	Mind. Verifikation E-Mail-Adresse oder Geschäftskundenvertrag	Mind. Verifikation E-Mail-Adresse oder Geschäftskundenvertrag
Identifikation Empfänger	Mind. Verifikation E-Mail-Adresse oder Geschäftskundenvertrag	Mind. Verifikation E-Mail-Adresse oder Geschäftskundenvertrag	Mind. Verifikation E-Mail-Adresse oder Geschäftskundenvertrag
Authentifikation Absender	Mind. E-Mail-Adresse und individuelles Passwort oder Domain-Zertifikat (GK-MGI*)	Mind. E-Mail-Adresse und individuelles Passwort oder Domain-Zertifikat (GK-MGI*)	Mind. E-Mail-Adresse und individuelles Passwort oder Domain-Zertifikat (GK-MGI*)
Authentifikation Empfänger	Mind. E-Mail-Adresse, verschlüsselte Nachricht und Sicherheitscode via E-Mail oder Domain-Zertifikat (GK-MGI*)	Mind. E-Mail-Adresse, verschlüsselte Nachricht und individuelles Passwort	Mind. E-Mail-Adresse, verschlüsselte Nachricht und individuelles Passwort oder Domain-Zertifikat (GK-MGI*)
Vertraulichkeit	Transportweg verschlüsselt GK-MGI*: im internen Netz des Geschäftskunden unverschlüsselt	Transportweg verschlüsselt GK-MGI*: Bei Versand im internen Netz des sendenden Geschäftskunden unverschlüsselt	Transportweg verschlüsselt GK-MGI*: im internen Netz des Geschäftskunden unverschlüsselt
Ausweisbare Nachrichtenstatus	Angekommen auf IncaMail Zugestellt Nicht zustellbar Systemnachricht Gelesen (nicht für GK-MGI*)	Angekommen auf IncaMail Zugestellt Nicht zustellbar Systemnachricht Gelesen	Angekommen auf IncaMail Angenommen Annahme verweigert Verfallen Nicht zustellbar
Protokollierung zwecks Nachvollziehbarkeit (Journal/Protokollbuch)	Status in online Logbuch oder Business Software	Status in online Logbuch oder Business Software	Status in online Logbuch oder Business Software Digital signierte Postquittungen für Abgabe und Empfang
Empfang	Web Interface Empfänger müssen Nachricht aktiv öffnen; GK-MGI* erhalten Nachricht automatisch.	Alle Empfänger müssen Nachricht aktiv öffnen.	Alle Empfänger müssen dem Empfang aktiv zustimmen.
Zustellung	Üblicherweise innerhalb weniger Sekunden. Bei Komplikationen: Mehrere Zustellversuche innerhalb 72 Std inkl. Information an Sender	Üblicherweise innerhalb weniger Sekunden. Bei Komplikationen: Mehrere Zustellversuche innerhalb 72 Std inkl. Information an Sender	Üblicherweise innerhalb weniger Sekunden. Bei Komplikationen: Mehrere Zustellversuche innerhalb 72 Std inkl. Information an Sender
Rechtliche Basis	AGB oder Geschäftskundenvertrag	AGB oder Geschäftskundenvertrag	AGB oder Geschäftskundenvertrag VeÜ-ZSSV**
Weiteres	-	-	Annahme kann durch Empfänger verweigert werden.

* GK-MGI = Geschäftskunden mit Mail Gateway Integration (MGI). Siehe Kapitel 3.1.

**Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren (VeÜ-ZSSV)

7 Zertifizierung und Verpflichtungen

Die Informationssicherheit von IncaMail basiert auf der zertifizierten Einrichtung eines Informations-Sicherheits-Management-Systems (ISMS) nach ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems – Requirements).

Weiter ist die Post CH Kommunikation AG in der Schweiz gemäss den gesetzlichen Anforderungen staatlich als offiziell zugelassene Zustellplattform für den elektronischen Rechtsverkehr in Verfahren vor Gerichten und Behörden (eGov) anerkannt worden. Die Akkreditierung als anerkannte Zustellplattform setzt neben der Erfüllung von Anforderungen an die Architektur und technische Sicherheit auch die Erfüllung hoher betrieblicher Anforderungen (Informationssicherheit und IT Service Management) voraus.

Die Post CH Kommunikation AG ist im Umgang mit Kundendaten an das Schweizerische Post- und Fernmeldegeheimnis gebunden und gewährleistet rund um IncaMail zum Beispiel auch den in der schweizerischen Bankenwelt, im Versicherungswesen oder in der Anwaltschaft vorgeschriebenen Vertraulichkeitslevel (Bankengeheimnis, Effektenhändlergeheimnis, Versicherungsgeheimnis, Anwaltsgeheimnis).

8 Einsatz von IncaMail in Europa

IncaMail steht weltweit bei zahlreichen Firmen im Einsatz. IncaMail zeichnet sich u.a. dadurch aus, dass die Verarbeitung der Daten in der Schweiz unter Einhaltung der Schweizer und Europäischen Datenschutzregulierung und strenger Informations- und Datensicherheitsmassnahmen erfolgt.

Die Europäische Kommission hat die Angemessenheit des Datenschutzniveaus in der Schweiz in aller Form bestätigt. Die Schweiz ergreift mit der Annahme des Änderungsprotokolls zur Datenschutzkonvention 108 des Europarats und der Revision des Datenschutzgesetzes die regulatorischen Massnahmen, um die Angemessenheit auch in Zukunft sicher zu stellen.

Für Kunden im Anwendungsbereich der DSGVO stehen für IncaMail die nötigen Datenschutzinstrumente (z.B. DPA) zur Verfügung.

9 Technische und organisatorische Massnahmen

Die für IncaMail eingesetzten IT-Systeme und weiteren Ressourcen werden durch technische und organisatorische Massnahmen der Informations- und Datensicherheit gegen unbefugtes Bearbeiten geschützt.

Die Post CH Kommunikation AG Bereich IncaMail hat durch technische und organisatorische Massnahmen ihre innerbetriebliche Organisation in einer den besonderen Anforderungen der Informationssicherheit gerecht werdenden Weise zur Sicherung aller sensitiven Daten vor Missbrauch gestaltet. Diese auf die Post CH Kommunikation AG Bereich IncaMail bezogenen Erläuterungen und Beschreibungen bilden in ihrer jeweils aktuellen Fassung einen Bestandteil der Dokumentation zur Informationssicherheit.

Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen sensitive (insbes. personenbezogene) Daten verarbeitet oder genutzt werden.

Massnahmen der Post CH Kommunikation AG Bereich IncaMail zur Zutrittskontrolle:
Die IncaMail-Server stehen in einem Rechenzentrum, welches über ein mehrstufiges Sicherheitskonzept verfügt und nach dem Raum-im-Raum-Prinzip gebaut ist.

Zu den Sicherheitsmerkmalen gehören:

- Das Rechenzentrum wird durch Kameras überwacht und rund um die Uhr (24/7) durch Sicherheitspersonal bewacht, welches die Gebäude innen und aussen kontrolliert
- Alle Gebäudebereiche sind alarmgesichert
- Ohne Identitätsnachweis kann niemand das Gebäude betreten oder verlassen, alle Besucher werden mit einer kundenspezifischen Berechtigungsliste abgeglichen

- Die Sicherheitssysteme umfassen kontaktlose Schlüsselkarten, die üblicherweise durch biometrische Lesegeräte und Personenvereinzelungsanlagen ergänzt werden

Zugangskontrolle

Ziel der Zugangskontrolle ist es, mit Hilfe geeigneter Massnahmen zu verhindern, dass Unbefugte Datenverarbeitungssysteme, mit denen sensitive (insbes. personenbezogene) Daten verarbeitet oder genutzt werden, nutzten können.

Massnahmen der Post CH Kommunikation AG Bereich IncaMail zur Zugangskontrolle:
Für administrative Tätigkeiten müssen sich die Operatoren über ein VPN an einem Jumphost anmelden und können dann nur von diesem auf die entsprechenden IncaMail-Server zugreifen. Die Authentifizierung am VPN findet über eine beidseitige zertifikatsbasierte Authentifikation statt. Die dann zu erfolgende Anmeldung am Jumphost erfordert eine SuisseID (fortgeschrittenes Zertifikat auf einem Hardware-Token). Danach muss sich der Operator am IncaMail-Server nochmals unter seiner UserID anmelden. Die jeweiligen Operatoren werden von der Post CH Kommunikation AG entsprechend autorisiert.

Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, zu gewährleisten, dass nur die zur Benutzung der Datenverarbeitungssysteme Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden sensitive (insbes. personenbezogene) Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Massnahmen der Post CH Kommunikation AG Bereich IncaMail zur Zugriffskontrolle
Die Zugriffe werden auf den jeweiligen Systemen protokoliert. Diese Protokolle werden gemäss Geschäftsbücherverordnung archiviert.

Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass sensitive (insbes. personenbezogene) Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Massnahmen der Post CH Kommunikation AG Bereich IncaMail zur Weitergabekontrolle:
IncaMail ist eine Plattform für den vertraulichen und nachweisbaren E-Mail Austausch. Dabei werden sowohl die Sender als auch die Empfänger der E-Mails identifiziert und authentifiziert.
Um sowohl die unterschiedlichen Anbindungsarten als auch die Prüfung auf Schadsoftware zu unterstützen, befinden sich Inhaltsdaten im Rahmen des Versand- und Leseprozesses temporär auf der Plattform. Selbstverständlich werden diese nach Abschluss dieser Versand- resp. Leseprozesse umgehend wieder entfernt. Auch sorgen die ISO 27001 zertifizierten Prozesse dafür, dass während dieser Versand- und Leseprozesse kein Unberechtigter (z.B. Administrator) Zugriff hat. Die Account- und Transaktionslogdaten werden auf verschlüsselten Backup-Devices aufbewahrt.

Eingabekontrolle

Ziel der Eingabekontrolle ist es, dass nachträglich festgestellt werden kann, ob und von wem sensitive (insbes. personenbezogene) Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Massnahmen der Post CH Kommunikation AG Bereich IncaMail zur Eingabekontrolle:

Jeder Teilnehmer an der IncaMail-Plattform wird identifiziert und authentifiziert. Die entsprechenden Tätigkeiten werden protokoliert.

Die Tätigkeiten der Operatoren der IncaMail-Plattform werden protokoliert.

Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass sensitive (insbes. personenbezogene) Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Massnahmen der Post CH Kommunikation AG Bereich IncaMail zur Auftragskontrolle:

Der Sender markiert jedes IncaMail mit einer von ihm gewünschten Versandart. Diese Versandart legt fest, wie die IncaMails zu verarbeiten sind. Diese Verarbeitung wird über die SW gesteuert.

Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass sensitive (insbes. personenbezogene) Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Massnahmen der Post CH Kommunikation AG Bereich IncaMail zur Verfügbarkeitskontrolle:

Die Infrastruktur ist redundant aufgebaut und die Account- und Transaktionslogdaten werden gebackupt. Die verschlüsselten Backups werden in einem Safe bei einer Schweizer Bank hinterlegt.

Trennungskontrolle

Ziel der Trennungskontrolle ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Zweckbindung).

Massnahmen der Post CH Kommunikation AG Bereich IncaMail zur Trennungskontrolle:

IncaMail läuft auf dedizierten Servern.

10 Umgang mit IncaMail

Als Plattform für den vertraulichen und nachvollziehbaren Informationsaustausch ist IncaMail eingebettet in ein Gesamtsystem (Mensch, Computer und Internet) von Sendern und Empfängern, wobei deren Sicherheit ausserhalb den Kontrollmöglichkeiten von IncaMail liegen.

Als Benutzer können Sie jedoch die Sicherheit dieses Gesamtsystems beeinflussen:

- Mensch:
  - Achten Sie auf ein sicheres Passwort für den IncaMail Service resp. Ihren E-Mail-Dienst. Wählen Sie kein leicht erratbares Passwort. Tipps für sichere Passwörter finden Sie bei der Registration von IncaMail; bei der Eingabe des Passwortes wird neben dem Eingabefeld die Passwortstärke grafisch angezeigt.
  - Ihr Passwort ist persönlich und geben Sie es niemandem weiter. Verwenden Sie ggf. einen Passwortmanager zur sicheren Aufbewahrung Ihres Passwortes.
  - Stellen Sie sicher, dass die von Ihnen eingegebene Empfängeradresse (E-Mail) korrekt ist und Ihrem gewünschten Empfänger entspricht.
  - Achten Sie auf die Wahl der richtigen Versandart (z.B. braucht es für gewisse Gerichtseingaben zwingend die Versandart (Einschreiben).
  - Falls Sie grosse Anhänge versenden, nutzen Sie den Large-File-Transfer von IncaMail. Ist dies nicht möglich, empfiehlt es sich, vorgängig beim Empfänger abzuklären, welche Datenmenge maximal pro E-Mail empfangen werden kann. Hierbei ist zu berücksichtigen, dass durch die Verschlüsselung durch IncaMail die Nachricht vergrössert wirdKontrollieren Sie die von IncaMail ausgestellten Quittungen auf Ihre Richtigkeit.

- Computer:
  - Schützen Sie Ihren Computer mit einem Virenschutzprogramm und halten Sie Ihr Betriebssystem und auch Ihre Anwendungen auf dem neuesten Stand (weitere Hinweise finden Sie auf der Melde- und Analysestelle Informationssicherheit MELANI des Bundes). Melden Sie sich nach erfolgter Transaktion bei IncaMail korrekt ab (Link „Abmelden“) und leeren Sie den Browser-Cache, wenn Sie IncaMail über das Web (www.incamail.com) verwenden.

- Internet:
  - Besuchen Sie nur Webseiten, denen Sie vertrauen. Achten Sie beim Login auf die grüne Anzeige des Links im Browser. Beachten Sie die Hinweise des Bundes bezüglich sorgsamem Umgang beim Surfen im Internet.

Voraussetzung für jede sichere Online-Transaktion oder -Kommunikation ist der sorgfältige Umgang aller Beteiligten mit allen Elementen im Prozess. Das gilt im e-Banking genauso wie in der Anwendung von IncaMail.

11 Anhang

11.1 ISO27001 - Zertifikat

swiss safety center

Zertifikat

swiss safety center ISO/IEC 27001 certified system

Die Zertifizierungsstelle von Swiss Safety Center AG
bescheinigt, dass die Firma

Post CH Kommunikations AG
Wankdorfallee 4
CH-3030 Bern

Niederlassung:
Franklinstrasse 26
CH-8050 Zürich

DIE POST
LA POSTE
LA POSTA

für den Geltungsbereich

Entwicklung, Vertrieb und Betrieb in den Bereichen Digital Health und E-Government

ein **Informationssicherheitsmanagementsystem (ISMS)**
erfolgreich anwendet nach

ISO/IEC 27001:2013

Erklärung zur Anwendbarkeit:	21.09.2021
Registriernummer:	22-267-704
Erstzertifizierung:	16.11.2018
Rezertifizierung:	20.12.2021
Gültig ab:	01.12.2021
Gültig bis:	30.11.2024

Heinrich A. Bieler
Leiter der Zertifizierungsstelle

Wallisellen, 06.01.2022

Swiss Safety Center AG, Certifications
Richtistrasse 15, CH-8304 Wallisellen
Ein Unternehmen der SVTI-Gruppe, Mitglied des VdTÜV

IAF