BEGASOFT
Digitale Lösungen

BEGASOFT AG
Laupenstrasse 17
CH-3008 Bern
T +41 (0)31 384 08 33
info@begasoft.ch
www.begasoft.ch

Technische und organisatorische Massnahmen zum ISDS (TOM)

15 ISMS

Exportiert am 17. April 2024

Inhaltsverzeichnis

Dokumenteninformationen

Status	In Bearbeitung	Zur Überprüfung	✅ Definitve Fassung
Klassifikation	✅ Öffentlich	Intern	Vertraulich
Gültig ab	17 Apr 2024		
Verfasser	@ Reto Häfeli		
Prozessowner	@ Mike Möri		
Version	1.0		

1 Einleitung

Die BEGASOFT AG betreibt sämtliche eigenen IT-Systeme und auch die IT-Systeme aller Kunden und Partner im BEGASOFT Rechenzentrum (Region Bern). BEGASOFT nutzt hierbei die Rechenzentrums-Infrastruktur der Swisscom (Schweiz) AG - in einem der modernsten Rechenzentren Europas.

BEGASOFT unterhält ein Information Security Management System (ISMS) gemäss dem internationalen Sicherheitsstandard ISO/IEC 27001:2013 und verfügt über eine entsprechende Zertifizierung.

Die nachstehend aufgeführten Massnahmen beziehen sich auf die Datenbearbeitung in den Rechenzentren der BEGASOFT und gelten für alle Daten, die auf dieser Infrastruktur verarbeitet werden. Findet die Datenbearbeitung durch von der BEGASOFT beauftragte Dritte statt, sorgt die BEGASOFT mittels geeigneter vertraglicher Vereinbarungen dafür, dass die beigezogenen Dritten vergleichbare Massnahmen einhalten.

In den folgenden Kapiteln werden die technischen und organisatorischen Massnahmen von BEGASOFT im Sinne der schweizerischen Gesetzgebung in Bezug auf Informationssicherheit und Datenschutz erläutert.

2 Vertraulichkeit (C)

2.1 Zutrittskontrolle

2.1.1 Physische Massnahmen

- Das Rechenzentrum befindet sich im Wankdorfquartier in Bern. Von der Standortwahl, über die spezielle Bauweise, den physikalischen Schutzmassnahmen bis hin zu einem ausgefeilten Sicherheitskonzept bietet das Rechenzentrum ein Höchstmass an Schutz.
- Das Rechenzentrum steht auf einem geschützen Areal (Zutritt ausserhalb der Bürozeiten nur mit Badge)
- Das Grundstück, auf dem das Rechenzentrum steht, wird durch einen Sicherheitsdienst rund um die Uhr überwacht.
- Das Rechenzentrum ist mit einem Schutzzaun und einer Schleuse gesichert (Zutritt nur mit Badge)

- Das Rechenzentrum ist zudem gegen Umweltereignisse wie z.B. Erdbeben und Blitzeinschlag geschützt und bei der Standortwahl wurde berücksichtigt, weder in einer Flugschneise, noch einem Hochwassergebiet noch in einem Gebiet mit Gefahrentransporten zu sein.

2.1.2 Technische Massnahmen

- Der Sicherheitsdienst ist 7/24 vor Ort und leitet allfällige Alarme weiter.
- Der Zutritt zum Gebäude und den einzelnen Rechnerräumen ist über mehrere Stufen mit elektronischen und biometrischen Zutrittssystemen geschützt.
- Sämtliche Räume werden mit Videokameras überwacht und jeder Zutritt wird protokolliert.
- Die BEGASOFT Räume (Cubes) und die einzelnen Racks sind abgeschlossen und können nur durch von BEGASOFT autorisierte Personen geöffnet werden.

2.1.3 Organisatorische Massnahmen

- Empfang (nur RZ Wankdorf)
- Geschütztes Schliesssystem (Schlüsselverwaltungsprozess physisch/ elektronisch)
- Protokollierung der Schliessmittelabgabe und –Rücknahme
- Protokollierung der Besucher/ Zuko Workflowtool für Gäste
- Nur autorisiertes Personal mit konkretem Auftrag/ Geregelter Zugang für mandatierte Transporteure und weitere Geschäftspartner
- Sperrbereiche (bspw. Liftsteuerung/ Heizung/ Lüftung/ Klima/ Elektroverteiler/ Traforaum/Batterieraum etc.)
- Sorgfalt bei Auswahl des Personals

2.2 Zugangskontrolle

2.2.1 Technische Massnahmen

Operations

- BEGASOFT betreibt eine professionelle, redundante und gewartete Firewall-Infrastruktur, welche auch von Kunden/Partnern als Managed RZ-Dienstleistung genutzt werden kann.
- Es wird eine Standard BEGASOFT Firewall-Konfiguration mit den minimalen Anforderungen eingesetzt. Zusätzliche Kunden-Konfigurationen können BEGASOFT mitgeteilt werden. Weiterführende Firewall-Lösungen (eigene Firewall, Firewall-Maintenance etc.) können auf Anfrage angeboten werden.
- Permanentes Security Monitoring/ Periodisches Vulnerability Management
- Anti-Malware-Software Server/ Clients/ mobile Geräte
- Intrusion Detection/Prevention IDS/IPS bzw. (Angrifferkennung und Verhinderung) dient der Erkennung und von Verhinderung von Angriffen, die gegen ein IT-System gerichtet sind.
- Externe Angriffe auf das System (Hacker, Malware, DDOS-Attacken) etc. werden protokolliert und nach Möglichkeit verhindert. Weiterführende IDS/IPS-Lösungen können auf Anfrage angeboten werden.
- BEGASOFT setzt auf ihren öffentlichen IP-Adressen eine professionelle DDoS-Schutz-Lösung ein.
- BEGASOFT betreibt eine professionelle und gewartete SPAM- und Viren-Filter Infrastruktur, welche auch von Kunden/ Partnern genutzt werden kann.

Identity and Access Management (IAM)

- Rechtevergabe- und Entzugsprozess (Eintritts-/Austrittsprozess
- Login mittels Benutzer-ID und Passwort, automatische Protokollierung des Zugangs
- Administrative/ sensitive Zugriffe mit 2FA und ausschliesslich verschlüsselt
- Remote-Zugriffe mittels VPN und 2FA (App oder SMS)

- WLAN: Sicherheit WPA2 PSK
- Accountsperrung nach 6 Fehlversuchen
- Zurücksetzung von Passwörtern anhand eines definierten Prozesses mit Protokollierung
- Automatische Sperrung der Clients nach festgelegtem Zeitablauf ohne Useraktivität
- Passwortspeicherung nur mit sicherem Hashingverfahren und Passwort-Tool
- Passwortänderung erzwungen: 90 Tage, letzte 12 Passwörter gesperrt
- Festplattenverschlüsselung (Bitlocker/FileVault)

2.2.2 Organisatorische Massnahmen

- Richtlinie Identity und Access Management
- Richtlinie Arbeitsplatz (Passwortdefinition)
- Richtlinie Firewall
- Richtlinie Mobile Computing und Telearbeit
- Richtlinie Change- und Patchmanagement

2.3 Zugriffskontrolle/ Eingabekontrolle

2.3.1 Technische Massnahmen

- Zuordnung jedes Accounts zu einer eindeutigen Identität
- Segregation of Duties (SoD, Funktionstrennung)
- Standard-Berechtigungsprofile auf Basis «need-to-know»/ Restriktive Handhabung privilegierter Zugriffe/ Periodische Rezertifizierung der AD-Rollen (insb. der privilegierten Rollen)
- Applikatorisches Logging zur Überwachung des Betriebs und zur Fehlersuche
- Dediziertes Benutzerprozessmanagement (abgestufte Berechtigungen) zur Gewährleistung von Nachvollziehbarkeit und Auskunftsfähigkeit
- Physische Vernichtung von Datenträgern und Quittierung der Vernichtung
- Nicht reversible Löschung von Datenträgern

2.3.2 Organisatorische Massnahmen

- Die Zugangs- und Zugriffskontrolle auf Ebene Server und Applikation wird durch die Applikationsanbieter (BEGASOFT oder Partner des Kunden) sichergestellt. Hierfür kommen Technologien wie Benutzerprofile und Benutzerrechte, IP-Security, VPN, SSL, 2FA etc. zur Anwendung.
- Vorgabe Clean Desk Policy
- Vorgabe Klassifizierung von Informationen
- Daten in Papierform werden mittels Aktenvernichter entsorgt. Datenträger, die aufbewahrt werden müssen, werden in einer sicheren Umgebung (Safe) gelagert. Zu entsorgende HW wird durch eine spezialisierte Firma entsorgt. Sämtliche Datenträger werden dabei aus den Geräten entfernt und im Beisein von BEGASOFT vor Ort mechanisch geschreddert und protokolliert.

2.4 Trennungskontrolle

2.4.1 Technische Massnahmen

- BEGASOFT setzt bei allen Kundenprojekten wo erforderlich, ein Zonenkonzept ein, welches unerlaubte Zugriffe verhindert (DMZ, LAN, SEC usw.). Ein Maleware Vorfall kann somit auf eine Zone isoliert werden.
- Einsatz von Firewalls mit kontinuierlicher Aktualisierung
- Trennung von Produktions- Integrations- und Testumgebung (PIT)
- Verwendung von Testdaten/ teilweise Maskierung/ Pseudonymisierung und Anonymisierung
- Physikalische- bzw. geografische Trennung von Systemen/ Datenträgern

- Logische Trennung von Systemen Datenträgern

2.4.2 Organisatorische Massnahmen

- Berechtigungs- und Rollenkonzept

3 Integrität (I)

3.1 Weitergabekontrolle

3.1.1 Technische Massnahmen

- Sensitive Datenübertragungen werden mit VPN oder TLS/SSL verschlüsselt, so dass eine abhör- und manipulationssichere Kommunikation zwischen den VPN-Partnern gewährleistet ist.
- Elektronische Signatur (evidience eSignature Solution)
- Einsatz von VPN (Client-VPN/ S2S)
- Sicherer Datentransport (SSL/TLS, SFTP)
- Festplattenverschlüsselung (Bitlocker/Filevault)
- Dediziertes Benutzerprozessmanagement (abgestufte Berechtigungen) zur Gewährleistung von Nachvollziehbarkeit und Auskunftsfähigkeit

3.1.2 Organisatorische Massnahmen

- Die Themen Datenschutz und Geheimhaltung sind in den 'Allgemeine Geschäftsbedingungen für Rechenzentrums-Dienstleistungen' (AGB-RZ) beschrieben bzw. geregelt. Die AGB-RZ sind für sämtliche betriebene IT-Systeme Vertragsbestandteil.
- Massnahmen zur Datenintegrität und der nachträglichen Nachvollziehbarkeit (wer hat welche Daten manipuliert) werden durch die Applikationsanbieter (BEGASOFT oder Partner des Kunden) sichergestellt. Hierfür kommen Technologien wie Versionierung, Historisierung, Intrusion Detection & Prevention (IDS/ISP) etc. zur Anwendung.
- Sorgfalt bei Auswahl von Personal
- Persönliche Übergabe mit Protokoll und Quittierung
- Vorgabe Remote-Zugriffe/ Fernwartung
- Vorgabe Mobile Device Management

4 Verfügbarkeit (und Belastbarkeit) (A)

4.1 Verfügbarkeitskontrolle

4.1.1 Technische Massnahmen

- Grundsätzlich steht die BEGASOFT RZ-Infrastruktur 7x24h (Verfügbarkeit: 99.9%) zur Verfügung. Service- bzw. Wartungsfenster werden in Absprache mit dem Kunden vereinbart.
- Doppelt gesicherte Steuerung: Die Energie- und Kommunikationsleitungen sowie die Klimasysteme sind redundant geführt (2-Weg)
- Die Stromversorgung erfolgt durch zwei unabhängige Hauseinführungen von zwei verschiedenen Versorgungszentralen des Stromlieferanten.
- Die unterbrechungsfreie Stromversorgung ist mit mehreren hochmodernen No-Break-Anlagen gewährleistet, die wöchentlich (Dieseltest), monatlich (Lasttest) und jährlich (vollständiger Stromausfalltest) getestet werden.

- Hochverfügbares neuartiges hybrides und äusserst ökologisches Kühlsystem mit Verdunstungskühlung unter Verwendung von Regenwasser sowie Abwärmenutzung.
- Das BEGASOFT Rechenzentrum ist über verschiedene, am Objekt örtlich getrennte Glaskabeleinführungen erschlossen. Mehrere unabhängige Serviceprovider (ISP's) sind mit Diensten im Rechenzentrum präsent und können genutzt werden. 'Multihomed-Internet-Konfigurationen' (BGP Lösungen) sind installiert und können nach Bedarf mitbenützt werden. BEGASOFT stellt die Überwachung und das Monitoring dieser Netzwerkanbindungen sicher. Dedizierte Netzwerkverbindungen (Mietleitungen) sind in verschiedenen Varianten und zugehörigen SLA's möglich.
- Der Brandschutz erfolgt durch eine Staub- und Brandfrüherkennungs-Anlage mit mehrstufiger Alarmierung an 7x24h vor Ort befindliches Sicherheitspersonal.
- Eigener Server-Raum, der als separater Brandabschnitt ausgelegt und mit einer modernen Brandlöschanlage ausgestattet ist.
- Die Brandbekämpfung erfolgt mit einer vollautomatischen Novec 1230 Löschanlage. Die Wirkung von Novec 1230 beruht auf seiner Eigenschaft, der Flamme beim Löschvorgang so viel Wärme zu entziehen, dass deren Temperatur unter den Wert sinkt, der für das Aufrechterhalten der Verbrennung erforderlich ist. Novec 1230 ist rückstandsfrei, beim Löschen erfolgt kein Rückstand und keine Sichtbehinderung. Novec 1230 ist ideal für den Schutz von Vermögenswerten, Computer- / EDV- und Telekommunikationsanlagen, Serverräumen, Labors, Archiven, Museen und Kunstgalerien.
- BEGASOFT betreibt eine professionelle und gewartete Überwachungs- und Alarmierungs-Infrastruktur, welche die BEGASOFT IT-Infrastruktur überwacht und als Managed RZ-Dienstleistung auch von Kunden/Partnern genutzt werden kann.
- Sämtliche technische Systeme (Server, Storage, Netzwerk etc.) werden permanent von dafür zuständigen Spezialisten gewartet.
- Regelmässige full- und incremental Backups
- Offline-Backups (örtlich getrennte Datenaufbewahrung)
- Verschlüsselte Backups
- Regelmässige Recovery-Tests und Protokollierung der Ergebnisse

4.1.2 Organisatorische Massnahmen

- Ein Backup- & Recovery Konzept umfasst die externe Datensicherung an einem sicheren Ort (BEGASOFT Rechenzentrum 2) und gewährleistet den Schutz personenbezogener Daten gegen zufällige Zerstörung oder Verlust. Das Backup- & Recovery Konzept bzw. die verlässliche Datenwiederherstellung wird regelmässig überprüft.
- Für den Desaster-Fall (Vorfall, welcher den Rechenzentrumsbetrieb am Standort Wankdorf verunmöglicht) besteht ein Notfallplan zur Inbetriebnahme eines vorbereiteten Backup-Standorts (BEGASOFT Rechenzentrum 2). Siehe auch 'Notfallplan' und 'Datenbackup & -Recovery'
- Freigabeverfahren für neue Software (Prozess Security Change/ Patchmanagement)
- Sicherheitskonzept für Software- und IT-Anwendungen
- Absolvierte Notfallübungen
- Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitenden

5 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

5.1 Datenschutz-Management

Im Rahmen der Leistungserbringung gegenüber ihren Kunden ist die BEGASOFT der verantwortungsvolle und rechtskonforme Umgang mit Personendaten ein grosses Anliegen. Die BEGASOFT stellt dabei sicher, dass die Daten mit grosser Sorgfalt und gemäss den einschlägigen gesetzlichen Bestimmungen des Datenschutzrechts behandelt werden. Die BEGASOFT verfügt über ein umfassendes Datenschutzmanagementsystem und prüft jede Dienstleistung auf ihre Datenschutzkonformität.

5.1.1 Technische Massnahmen

- BEGASOFT betreibt eine professionelle und gewartete Überwachungs- und Alarmierungs-Infrastruktur, welche die BEGASOFT IT-Infrastruktur überwacht und als Managed RZ-Dienstleistung auch von Kunden/Partnern genutzt werden kann.
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf
- Zertifizierungen: ISO/IEC 9001 und ISO/IEC 27001
- Mindestens jährliche Überprüfung der Wirksamkeit der technischen Schutzmassnahmen
- Datenschutz Management System mit unterstützenden Tool-Lösungen (Schnittstellenverwaltung, Bearbeitungsverzeichnisse etc.)

5.1.2 Organisatorische Massnahmen

- Es existiert ein Notfallplan, welcher bei Major- und Security-Incidents zur Anwendung kommt. Der Notfall wird periodisch (2x jährlich) getestet bzw. durchexerziert.
- Im Rahmen der ISO 9001- und ISO 27001-Prozesse überwacht ein BEGASOFT-interner Sicherheits- und Datenschutzbeauftragter sämtliche vorgesehenen ISDS-Massnahmen.
- BEGASOFT RZ-Mitarbeiter unterliegen strengen vertraglich geregelten Geheimhaltungsvereinbarungen und werden regelmässig (4x jährlich) zu Sicherheits-, Notfall- und Geheimhaltungs-Themen geschult.
- BEGASOFT hat diverse Security-Massnahmen wie Passwort-Richtlinien, Identifizierung von Kunden/Partnern und Dritten, 4-Augen-Prinzip etc. etabliert. Auf Wunsch und Anfrage können die Security-Massnahmen jederzeit durch berechtigte Kunden und/oder Partner vor Ort besichtigt und im Detail erläutert werden (siehe Kapitel Audits).
- Datenschutzleitbild
- Unternehmensweite Vorgaben zum Datenschutz (inkl. Ausführungsbestimmungen und zugehörigen Prozessen)
- Regelmässige Schulung der Mitarbeitenden
- Verpflichtung der MA zur Geheimhaltung
- Durchführung von Datenschutz-Folgenabschätzungen (DSFA) abgebildet in der Risikomatrix
- Gewährleistung der Informationspflichten
- Formalisiertes Leitbild zur Bearbeitung von Auskunftsanfragen sowie weiteren Rechten von Betroffenen
- Verpflichtung der Mitarbeiter des Auftragnehmers zu Geheimhaltung (NDA)
- Überbindung der Vorgaben zu Informationssicherheit und Datenschutz auf Auftragnehmer und allfällige Subunternehmer

5.2 Privacy- und Security by Design

5.2.1 Technische Massnahmen

- Anwendung unterschiedlicher Security-Tools im Rahmen der Softwareentwicklung
- Security Health-Checks für eigenentwickelte Software (automatisierte Prüfprozesse)

5.2.2 Organisatorische Massnahmen

- Umfassender Katalog von technischen Massnahmen für sichere Software-Entwicklung
- Einsatz von Security Champions (Security-affine Mitarbeitende mit vertieftem Wissen zu Informationssicherheit und Datenschutz
- Regelmässige Weiterbildungen zu Softwareentwicklung

6 Anhang (weitere Ausführungen)

6.1 Softwareentwicklung

Die BEGASOFT orientiert sich in der Softwareentwicklung an internationalen best practices und hat für jedes Projekt ein Mindest-Security-Setup etabliert. Risikobasiert werden in Abhängigkeit der Kritikalität betriebener Services oder Produkte weitere Sicherheitstests durchgeführt.

Die BEGASOFT setzt folgende Methoden zur sicheren Softwareentwicklung ein:

- Secure Code Review mit dem Ziel der Identifizierung von Fehlern, Defekten und Inkompatibilitäten zu Anforderungen oder Sicherheitsschwachstellen sowie der Verbesserung des Wissensmanagements.
- Static Application Security Testing (SAST) für die Prüfung des Quellcodes, der Binärdateien und des Bytecodes mit Abdeckung der meisten Programmiersprachen (White-Box-Tool)
- Dynamic Application Security Testing Tool (DAST) zur Erkennung der Bedingungen, welche auf Sicherheitslücken einer laufenden Anwendung hinweisen mit vertiefter Prüfung auf Eingabe- und Ausgabeschwachstellen (Black-Box-Tool)
- Software Composition Analysis (SCA) zur Analyse der Softwarezusammensetzung von Open Source Software inkl. transitiven Abhängigkeiten und zur Verwaltung der Lizenzen (FOSS)

Die BEGASOFT setzt im Rahmen der Softwareentwicklung unter anderem folgende Tools ein:

- Git/GitLab (Code Review inkl. standardisierte Checkliste bei Merge-Requests)
- SonarQube (SAST) → im Aufbau
- nuclei (DAST) → im Aufbau
- Dependency-Track (SCA)

6.2 Zertifizierungen

Auf Wunsch können die Massnahmen zur Thematik Informationssicherheit und Datenschutz jederzeit durch berechtigte Kunden und/oder Partner vor Ort besichtigt und im Detail erläutert werden.

6.2.1 BEGASOFT AG

ISO 9001:2015

ISO 9001 definiert international gültige Qualitätsmanagementnormen und hilft Unternehmen, eine gleichbleibende Qualität ihrer Produkte und Dienstleistungen zu garantieren.

ISO 27001:2013

Internationale Norm für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheits-Managementsystems (ISMS).

Informatik Strategieorgan Bund

BEGASOFT wurde 2003, 2006 und 2013 durch das Informatiksteuerungsorgan des Bundes ISB bez. Informationssicherheit auditiert und hat die Audits erfolgreich bestanden. BEGASOFT betreibt rund 60 IT-Systeme für diverse Organisationen der Öffentlichen Hand (Referenzliste auf Anfrage) und IT-Systeme für diverse namhafte Kunden mit zum Teil hochsensitiven Daten.

6.2.2 Rechenzentrum Bern Wankdorf

Das BEGASOFT Rechenzentrum Bern Wankdorf ist als eines von ganz wenigen Rechenzentren in Europa und als einziges Rechenzentrum in der Schweiz (dies sowohl für Design als auch Construction) Tier IV zertifiziert. Weiter ist das Rechenzentrum ISO 9001, 14001, 15504 und 27001 zertifiziert und besitzt mit myclimate ein Umweltlabel für besonders klimafreundliche Produkte und

Dienste. Dazu wird jährlich das Rechenzentrum nach ISAE 3000 (Type 2) auditiert. Der PUE-Wert (Power Usage Effectiveness) beträgt 1.25.

6.3 Audits

Audits durch Kunden oder durch von Kunden beauftragte Dritte können in Absprache mit BEGASOFT und unter Kostenfolge für die Kunden vereinbart und durchgeführt werden. BEGASOFT behält sich bei Audits vor, mit Kunden oder dem von Kunden beauftragten Dritten eine Geheimhaltungsvereinbarung abzuschliessen.