

BEGASOFT AG
Chutzenstrasse 24
CH-3007 Bern

T +41 (0)31-398 08 33
F +41 (0)31-382 43 75

info@begasoft.ch
www.begasoft.ch

BEGASOFT ISDS (Informationssicherheit und Datenschutz) -Massnahmen

Version 2.8
3. Januar 2018



Inhaltsverzeichnis

1	BEGASOFT Sicherheitspolitik	3
2	BEGASOFT ISDS (Informationssicherheit und Datenschutz) -Massnahmen	4
2.1	Technische Massnahmen	4
2.2	Organisatorische Massnahmen	6
2.3	Zertifizierungen / Audits	7

1 BEGASOFT Sicherheitspolitik

Die BEGASOFT AG betreibt seit Frühling 2015 sowohl sämtliche eigenen IT-Systeme als auch die IT-Systeme aller Kunden und Partner im neuen BEGASOFT Rechenzentrum Bern Wankdorf (Tier Level IV). BEGASOFT nutzt hier bei die Rechenzentrums-Infrastruktur der Swisscom (Schweiz) AG - in einem der modernsten Rechenzentren Europas.

Die RZ- und IT-Infrastruktur im BEGASOFT Rechenzentrum Bern Wankdorf sucht ihres gleichen und punkto Sicherheit, Verfügbarkeit und Ökologie profitieren BEGASOFT Kunden von allerhöchster Qualität.

BEGASOFT wurde 2003, 2006 und 2013 durch das Informatiksteuerungsorgan des Bundes ISB bez. Informationssicherheit auditiert und hat die Audits erfolgreich bestanden, zudem ist BEGASOFT ISO 9001:2008 und ISO 27001:2013 zertifiziert. BEGASOFT betreibt rund 60 IT-Systeme für diverse Bundesämter (Referenzliste auf Anfrage) und IT-Systeme für diverse namhafte Kunden mit zum Teil hochsensitiven Daten.

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

Die BEGASOFT Sicherheitspolitik (inkl. ISDS-Massnahmen) umfasst sämtliche Bereiche von BEGASOFT (keine Ausschlüsse gem. ISO 27001) und baut auf einer umfassenden und jährlich neu beurteilten Risikoanalyse auf. Unter Risiko versteht BEGASOFT 'Risikoidentifizierung', 'Riskobewertung', 'Risikomanagement' und Risikominimierung. Die Risiken in den Bereichen 'Höhere Gewalt', 'Organisatorische Mängel', 'Menschliche Fehlhandlungen', 'Technisches Versagen' und 'Vorsätzliche Handlungen' werden identifiziert, unter den Aspekten 'Verfügbarkeit', 'Vertraulichkeit', 'Integrität' und 'Nachvollziehbarkeit' bewertet und es werden entsprechende Massnahmen zur Risikominimierung ergriffen.

2 BEGASOFT ISDS (Informationssicherheit und Datenschutz) -Massnahmen

2.1 Technische Massnahmen

Rechenzentrum-standort Schweiz	Das BEGASOFT Rechenzentrum befindet sich im Wankdorfquartier in Bern. Von der Standortwahl, über die spezielle Bauweise, den physikalischen Schutzmassnahmen hin bis zu einem ausgefeilten Sicherheitskonzept bietet das Rechenzentrum ein Höchstmass an Schutz. 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 Gefahrtransporten zu sein. Das Grundstück, auf dem das Rechenzentrum steht, ist nachts gesichert und wird durch einen Sicherheitsdienst überwacht.
Brandschutz	Der Brandschutz erfolgt durch eine Staub- und Brandfrühsterkennungs-Anlage mit mehrstufiger Alarmierung an 7x24 vor Ort befindliches Sicherheitspersonal. 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.
Einbruch- und Zutrittsschutz	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. Der Sicherheitsdienst ist 7/24 vor Ort und leitet allfällige Alarmer weiter.
Unterbrechungsfreie Stromversorgung	Die Stromversorgung erfolgt durch zwei unabhängige Hauseinführungen von zwei verschiedenen Versorgungszentralen des Stromlieferanten. Die unterbrechungsfreie Stromversorgung ist mit hochmodernen No-Break-Anlagen gewährleistet, die wöchentlich (Dieseltest), monatlich (Lasttest) und jährlich (vollständiger Stromausfall Test) getestet werden.
Klimatisierung	Neuartiges hybrides Kühlsystem mit Verdunstungskühlung unter Verwendung von Regenwasser sowie Abwärmenutzung.
Netzwerkredundanz	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 mitbenutzt werden. BEGASOFT stellt die Überwachung und das Monitoring dieser Netzwerkanbindungen sicher. Dedizierte Netzwerkverbindungen (Mietleitungen) sind in verschiedenen Varianten und zugehörigen SLA's möglich.

Firewall- und Security-Infrastruktur BEGASOFT betreibt eine professionelle, redundante und gewartete Firewall-Infrastruktur, welche auch von Kunden/Partnern als Managed RZ-Dienstleistung genutzt werden kann. Gewünschte Konfigurationen können BEGASOFT mitgeteilt werden. Weiterführende Firewall-Lösungen (eigene Firewall, Firewall-Maintenance etc.) können auf Anfrage angeboten werden.

Intrusion Detection/Prevention (IDS/IPS) bzw. Angriefferkennung 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.

SPAM- und Virenschutz BEGASOFT betreibt eine professionelle und gewartete SPAM- und Viren-Filter Infrastruktur, welche auch von Kunden/Partnern genutzt werden kann.

Datenübertragung Sensitive Datenübertragungen werden mit VPN oder TLS/SSL verschlüsselt, so dass eine abhör- und manipulationssichere Kommunikation zwischen den VPN-Partnern gewährleistet ist.

Patch-Management Sämtliche technischen Systeme (Server, Storage, Netzwerk etc.) wird permanent von dafür zuständigen Spezialisten gewartet.

Überwachung und Alarmierung 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.

Verfügbarkeit RZ-Infrastruktur Grundsätzlich steht die BEGASOFT RZ-Infrastruktur 7x24h (Verfügbarkeit: 99.8%) zur Verfügung. Service- bzw. Wartungsfenster werden in Absprache mit dem Kunden vereinbart.

2.2 Organisatorische Massnahmen

Notfallplan	Es existiert ein Notfallplan, welcher bei Major- und Security-Incidents zur Anwendung kommt. Der Notfall wird periodisch getestet bzw. durchexerziert.
Sicherheits-beauftragter	Im Rahmen der ISO 9001- und ISO 27001-Prozesse überwacht ein BEGASOFT-interner Sicherheits- und Datenschutzbeauftragter die vorgesehenen Massnahmen.
Personal	BEGASOFT RZ-Mitarbeiter unterliegen vertraglich geregelten Geheimhaltungsvereinbarungen und werden regelmässig zu Sicherheits-, Notfall- und Geheimhaltungs-Themen geschult.
Security-Massnahmen	BEGASOFT hat diverse Security-Massnahmen wie Zutrittskontrolle in die Räumlichkeiten, Passwort-Richtlinien, Identifizierung von Kunden/Partnern und Dritten, 4-Augen-Prinzip etc. etabliert. Auf Wunsch und Anfrage können die Security-Massnahmen jederzeit durch berechnigte Kunden und/oder Partner vor Ort besichtigt und im Detail erläutert werden.
Datenschutz, Geheimhaltung sowie Daten-integrität	<p>Die Themen Datenschutz und Geheimhaltung sind in den 'Allgemeine Geschäftsbedingungen für Rechenzentrums-Dienstleistungen' (AGB-RZ) sowie in den Service Level Agreements (SLA) beschrieben bzw. geregelt. Die AGB-RZ sind für sämtliche betriebene IT-Systeme Vertragsbestandteil.</p> <p>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.</p>
Zugangs- und Zugriffskontrolle	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, Zwei-Faktor-Authentifizierung etc. zur Anwendung.
Datenbackup & -Recovery	Ein Backup- & Recoverykonzept umfasst die externe Datensicherung an einem sicheren Ort (BEGASOFT Rechenzentrum 2) und gewährleistet den Schutz personenbezogener Daten gegen zufällige Zerstörung oder Verlust. Das Backup- & Recoverykonzept bzw. die Datenwiederherstellung wird regelmässig überprüft.
Disaster-Szenario	Für den Disaster-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'
Datenträger-Entsorgung	Daten in Papierform werden mittels Aktenvernichtern entsorgt. Datenträger die aufbewahrt werden müssen, werden in einer sicheren Umgebung (Safe) gelagert. Zu entsorgende HW wird durch die Firma Swico (http://www.swicorecycling.ch/de/home) entsorgt. Sämtliche Datenträger werden dabei aus den Geräten entfernt und im Beisein von BEGASOFT vor Ort mechanisch geschreddert.

2.3 Zertifizierungen / Audits

BEGASOFT ist seit 2013 ISO 9001- und seit 2015 ISO 27001-zertifiziert.

BEGASOFT wurde 2003, 2007 und 2013 vom ISB (Informatik Strategieorgan Bund) auditert und befähigt, IT-Systeme für Bundesämter zu betreiben. Diverse IT-Systeme für Bundesämter (> 50) werden im BEGASOFT AG Rechenzentrum betrieben.

Das BEGASOFT Rechenzentrum Bern Wankdorf ist als eines von ganz wenigen Rechenzentren in Europa und als einziges Rechenzentrum in der Schweiz Tier IV (dies sowohl für Design als auch Construction) zertifiziert. Weiter ist das Rechenzentrum ISO 9001, 14001, 15504 und 27001 zertifiziert und besitzt mit myclimate ein Umweltlabel für besonders klimafreundliche Produkte und Dienste. Der PUE-Wert (Power Usage Effectiveness) beträgt 1.25.

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