archivsuisse
sicher I kompetent I persönlich

Sicherheitskonzepte

1. **Archivräume Aathal und Uster**
2. **Sicherheits- + Notfallkonzept IT**
3. **Sicherheitskonzepte Transport**
4. **Business Continuity Management**

archivsuisse c/o Bubu AG, 8606 Uster

Stand August 2019

archivsuisse c/o Bubu AG
Wermatswilerstrasse 8b, 8610 Uster
T +41 (0)44 940 35 70, F +41 (0)44 949 44 55
zh@archivsuisse.ch, www.archivsuisse.ch

1. Sicherheitskonzept Archivräume Aathal und Uster

Standorte, Zugänglichkeit	Die Räume liegen in einem ehemaligen Lebensmittellager der Armee im Aathal (4 Archivräume) sowie in einem ehemaligen Käselager in Uster (1 Archivraum). Beide Gebäude liegen ausserhalb der vom Amt für Wasser, Energie und Luft (AWEL) des Kantons Zürich definierten Hochwassergefahrenzone und sind für Transportfahrzeuge zugänglich (Abladerampe).
Lage im Gebäude	Die Räume liegen im Aathal im 1. Obergeschoss sowie im Erdgeschoss und in Uster im 2. Untergeschoss. Sie weisen keine Fenster auf und haben überschaubare Zugänge (pro Archivraum: 1 Haupttor und 1 Notausgang). Die Räume sind für Stapler zugänglich.
Gebäudehülle	Die Gebäude sind massiv gebaut. Die Wände sind aus Stahlbeton.
Boden	Der Boden ist für hohe Nutzlasten ausgelegt und unbehandelt.
Klima, Bandbreiten	Die Raumtemperatur bewegt sich in einer Bandbreite von 7°-24°C bei einer relativen Luftfeuchtigkeit von 40%-57%. Die Stabilität und Grenzwerte der Luftfeuchtigkeit und der Raumtemperatur wird mit technischen Geräten (Luftentfeuchtungsanlage, Heizlüftung mit einem Wärmetauscher im Gebäude Aathal) sichergestellt. Die Schwankungen betragen nicht mehr als +/-2°C innerhalb von 24 Stunden. Die Luftentfeuchtungsanlage verfügt über Filter, die das Eindringen von Sporen und Insekten verhindern. Der Wärmetauscher befindet sich ausserhalb der Archivräume.

archivsuisse c/o Bubu AG
Wermatswilerstrasse 8b, 8610 Uster
T +41 (0)44 940 35 70, F +41 (0)44 949 44 55
zh@archivsuisse.ch, www.archivsuisse.ch

Klima, Kontrolle

Die Kontrolle des Raumklimas erfolgt mit drei Messfühlern pro Raum, die Daten via Funk in einem geschlossenen System übermitteln. Die Auswertung kann in Form von Grafiken (Kurven) oder Messtabellen einfach verfügbar gemacht werden. Die Daten werden regelmässig beobachtet. In Uster herrschen nach Langzeitmessung stabile Verhältnisse und es wird daher keine spezielle Messinfrastruktur benötig.

Sicherheit, Feuer

Die Räume entsprechen den hohen Anforderungen an den baulichen Brandschutz, d.h. Massivböden und -decken, Wände aus Stahlbeton, keine Bodenanstriche. Die Türen haben Brandschutz-Klassifikation EI30.

Die Luftentfeuchtungsanlagen im Gebäude Aathal sind durch Brandschutzklappen zwischen den Räumen getrennt.

Die Räume verfügen über automatische Brandmeldeanlagen.

In allen Räumen dürfen keine flüssigen und selbstentzündbaren oder chemischen Stoffe gelagert werden.

Sicherheit, Wasser

Nur in den Räumen im Aathal sind für die Beheizung notwendige Wasserleitungen vorhanden. Diese sind über einen Druckmesser im Heizsystem mit der Alarmanlage verbunden. Ein Druckabfall würde sofort die Notfallorganisation in Kraft setzten.

Archivgut der Sicherheitsstufe FINMA-Konformität wird im Aathal mit mind. 50 cm Bodenfreiheit gelagert.

Sicherheit, Einbruch

Im Aathal sind zwei der drei Haupttore und die Notausgänge mit Widerstandsklasse RC3 ausgestattet.
In Uster sind das Haupttor und der Notausgang mit der Widerstandsklasse RC3 ausgestattet.

Die Öffnung der einzelnen Haupttore wird mit protokollierter Zutrittskontrolle (batteriegestützt) per Code und Fingerprint gewährleistet.

Die Notausgänge sind permanent unter Alarm und werden nur in Notfällen geöffnet.

Die Räume sind videoüberwacht. und verfügen über eine Alarmanlage.

Gestelle:

Archivgut wird in Metallregalen aus einbrennlackiertem Stahl gelagert.

Arbeitsplatz

An jedem Standort ist befindet sich ein Arbeitsplatz für zugelassenes Personal für die Suche nach Dossiers und für Recherchen.

Alle Räume verfügen über ein verschlüsseltes W-LAN, um Barcodes in die Datenbank einzulesen.

In allen Archivräumen sind Chemikalien, Lebensmittel und Getränke verboten.

Pro Standort sind maximal 25 Liter destilliertes Wasser für den Betrieb der Elektrostapler zugelassen. Der Wasserbehälter wird in einer Auffangwanne gelagert.

Alarmierung

Die Alarmauslösung erfolgt bei unterschiedlichen Szenarien (Brand, Einbruch, Technische Störung/Sabotage, Druckabfall Heizung) über eine externe Alarmzentrale und über eine Szenario-orientierte Telefonkaskade (Leitung, Mitarbeiter Archiv, Feuerwehr, Polizei).

2. Sicherheits- und Notfallkonzept IT (Information Technology)

Sicherheitsziele

Sicherheitsziele sind

- Unversehrtheit der IT-Infrastruktur;
- Vermeidung resp. Behebung von technischen Störungen und Systemausfällen;
- Sicherheit der Daten vor Verlust und/oder Vernichtung;
- Disaster Recovery Management;
- Datenschutz und Vertraulichkeit (insbesondere bei Bankkunden- und Versicherungsdaten);
- Kein Eindringen auf die Systeme von aussen.

Grundlagen

Archivsuisse setzt für die Verwaltung der Metadaten der physisch archivierten Dossiers eine SQL-basierte Datenbank ein. Es handelt sich um eine Eigenentwicklung, die spezifisch auf die Archivierung ausgerichtet ist und sich an den ISAD(G)-Standards orientiert. Sie kann flexibel an Kundenbedürfnisse angepasst werden. Die Metadaten verschiedener Kunden sind getrennt in separaten Datenbanken gespeichert.

Archivsuisse bezieht für die Langzeitarchivierung elektronischer Daten im Auftrag von Kunden Dienstleistungen der netrics AG. Sowohl die Datenbank als auch die langzeitarchivierten Kundendaten befinden sich auf Servern der netrics AG. Diese verfügt über Rechenzentren an zwei verschiedenen Standorten in der Schweiz und ist nach ISO 9001:2008, ISO/IEC 20000-1:2011 und ISO/IEC 27001:2013 zertifiziert.

Unversehrtheit der IT-Infrastruktur

Eigene IT-Systeme von archivsuisse c/o Bubu AG werden durch die internen IT-Mitarbeitenden der Bubu AG beschafft, installiert und betreut.

Für die Langzeitarchivierung werden Kundendaten von archivsuisse in archivfähige Formate migriert und auf die von der netrics AG betreuten Systeme übertragen. Ursprüngliche Hard- und Software-Umgebungen werden nicht weiterbetrieben. Die Betreuung der Hardware wie auch der Betriebssysteme ist dementsprechend an die netrics AG ausgelagert und wird durch archivsuisse überwacht.

Vermeidung resp. Behebung von

Technische Störungen werden in den Rechenzentren durch optimale Umgebungsparameter weitestgehend vermieden (Klimatisierung, Brandschutz, Zutrittskontrolle, unterbuchsfreie Stromversorgung, etc.). Service Level und maximale Ausfallzeiten sind kundenspezifisch in den jeweiligen Prozessbeschrieben festgehalten.

Systemkritische Applikationen werden primär von eigenen Mitarbeitenden betreut und bei Bedarf mit Wartungsverträgen abgesichert. Die vorgeschriebenen Wartungsintervalle sind terminiert und deren Einhaltung wird kontrolliert.

Datensicherheit

Alle Server und relevanten Datenträger sind in abgeschlossenen Räumen mit einer Zutrittskontrolle oder einem strikten Schlüsselregime gesichert. Ebenfalls sind die Räume mit Bewegungsmeldern, Brandmeldern und Video überwacht.

Die Sicherheit der Daten vor Verlust und/oder Vernichtung wird mit einer dualen Datensicherung gewährleistet. Von der SQL-Datenbank mit den Metadaten wird einmal täglich ein internes Backup durch die IT der archivsuisse c/o Bubu AG erstellt. Ebenfalls wird einmal täglich eine Synchronisation mit den Servern der netrics AG durchgeführt, auf dem die Kunden mit ihrem Login

auf ihre Daten zugreifen können. Die Daten befinden sich stets an zwei getrennten Orten. Die Wiederherstellung der Daten ist im Verlustfall jederzeit aus den Backups möglich. Weitere geschäftsrelevante Daten werden zweimal täglich intern und einmal täglich extern gesichert.

Die Langzeitarchivierung von Kundendaten bei netrics AG erfolgt auf der Basis der Zertifizierungen ISO 9001:2008, ISO/IEC 20000-1:2011 und ISO/IEC 27001-2013. Darin enthalten sind Backups an zwei verschiedenen Standorten.

Disaster Recovery Management

Im Falle elementarer Schadenereignisse in den Büroräumen in Uster kann archivsuisse den Betrieb innerhalb von 12 Stunden in den Räumen der Bubu AG in Mönchaltorf wieder aufnehmen (Verweis: zur Sicherheit der physisch archivierten Dokumente siehe die separaten Sicherheitskonzepte für die Archivräume Uster bzw. Aathal).

Im Falle elementarer Schadenereignisse verfügt netrics AG über einen "Disaster Recovery Management"-Prozess. Dadurch wird sichergestellt, dass die Rechenzentren, die in den Service Levels kundenspezifisch vereinbarten Minimalanforderungen bereitstellen können. Die dokumentierten Prozesse sind interne und vertrauliche Dokumente und werden von den Rechenzentren nicht an externen Stellen abgegeben. Im Rahmen eines Audits ist eine Einsichtnahme vor Ort unter Begleitung gewährleistet.

Datenschutz und Vertraulichkeit

Archivsuisse ist GoodPriv@cy-zertifiziert und verfügt über ein Datenschutzkonzept, das auf der Webseite veröffentlicht ist. Darin festgehalten sind sowohl technische als auch organisatorische Massnahmen. Die Massnahmen richten sich nach dem need-to-know-Grundsatz. Mitarbeitende haben nur auf diejenigen Informationen Zugriff, die für die Wahrnehmung der jeweiligen Aufgaben erforderlich sind.

Die organisatorischen Massnahmen umfassen eine besondere Sorgfalt bei der Auswahl des Personals (Überprüfung der Strafregisterauszüge) sowie regelmässige Datenschutzschulungen, die die Mitarbeitenden für den Datenschutz und die Vertraulichkeit sensibilisieren. Alle Mitarbeitenden von archivsuisse haben eine Vertraulichkeitsvereinbarung unterzeichnet, die namentlich auf Art. 47 BankG und Art. 162 StGB aufmerksam macht.

Die technischen Massnahmen umfassen mehrere Sicherheitsschranken:

- Sämtliche Systeme, die archivsuisse einsetzt, sind passwortgeschützt.
- Alle User haben ein eigenes Login mit Passwort. Sensible Applikationen sind durch ein weiteres Login mit Passwort abgegrenzt.
- Das Login in die SQL-Datenbank ist zweistufig: Auf Login-Stufe erfolgt, mittels einer Kunden-ID, die Prüfung der Zugriffsberechtigung. Danach erfolgt die Eingabe des Passworts.
- In der SQL-Datenbank werden in den Metadaten keine besonders schützenswerten Personendaten erfasst. So werden im Sinne der Pseudonymisierung bei Patientendossiers und Bankkunden- resp. Versicherungsdossiers nur die Patienten- bzw. Kundennummern erfasst, aber keine Namen oder weiteren Daten, die eine Identifizierung einer Person ermöglichen könnten (auch nicht indirekt).

Eindringen auf die Systeme von aussen

Alle Systeme sind durch eine Firewall. Die Verbindungsmöglichkeiten sind auf das notwendige Minimum reduziert. Verbindungen zu externen Stellen und Arbeitsplätzen sind nur mit einer VPN-Verbindung zugelassen. Auf allen Geräten sind aktuelle Virenschutzprogramme installiert.

Bankensysteme, die Client Identifying Data (CID) enthalten, werden von allen übrigen Systemen getrennt betrieben. Der Zugriff auf CID ist nur für besonders berechtigte Mitarbeitende auf einem separaten, passwortgeschützten Rechner in den Räumen von archivsuisse in Uster möglich. An diesen Rechner dürfen weder private Geräte angeschlossen werden, noch verfügt er über eine Internet-Verbindung. Der Rechner verfügt ausschliesslich über eine SSL-verschlüsselte VPN-Anbindung für den Zugriff auf das Banken- resp. Versicherungssystem.

3. Sicherheitskonzept Transporte

Allgemeines:

Transporte werden mittels einem von zwei sicherheitsrelevanten Abläufen durch archivsuisse ausgeführt. Je nach Ablauf der Registratur (Erstellen eines Verzeichnisses über die Archivgüter) wird das Archivgut beim Kunden erfasst und in die–von archivsuisse bereitgestellten Transportboxen umgelagert, oder provisorisch verpackt und bei archivsuisse registriert. Weitere Variationen sind möglich. Beim Beladen des LKW ist immer eine Person auf der Ladebrücke stationiert.

Sicherheitsstufe Basis:

Das Archivgut wird in Transportbehälter (Palettenrahmen oder Grossboxen) umgelagert und mit dem eigenen Kleintransporter oder LKW mit einem Chauffeur in unsere Archivräume transportiert.

Sicherheitsstufe Hoch/FINMA:

Das Archivgut wird in Transportbehälter (Palettenrahmen oder Grossboxen) umgelagert und vergittert mit dem eigenen Kleintransporter oder dem LKW mit Hardtop in unsere Archivräume transportiert. Neben dem Chauffeur wird der Transport durch eine Begleitperson von archivsuisse oder dem Kunden begleitet.

Spezielle Sicherheitsstufen

Die Sicherheitsstufen können auf Kundenanforderung weiter erhöht werden (z.B. separate Begleitfahrzeug, zusätzliches Sicherheitspersonal).

4. Business Continuity Management

Alternative Site

Im Falle von Elementarschäden in den Büros in Uster kann innerhalb von 12 Stunden der operative Betrieb in den Räumlichkeiten der Bubu AG in Mönchaltdorf wiederaufgenommen werden.

Vitale Geschäftsprozesse:

Alle für die operative Weiterführung der Auskunftsbereitschaft zu den Beständen notwendigen (vitalen) Informationen sind auch ausserhalb der Räumlichkeiten (bei der Bubu AG, Standort Bern, Providern z.B. Kundenportal) verfügbar.

Notfallorganisation:

Über das Alarmierungssystem ist die Kommunikation zwischen Schlüsselpersonen sichergestellt und die sofortige Situationsanalyse und Definition von Notfallmassnahmen sind innert weniger Stunden möglich.

Vorkehrungsmassnamen

Die Notfallvorkehrungen der Archivräume umfassen regelmässige Schulungen der Mitarbeiter mit dem Umgang und das richtige Verhalten bei Elementarschäden (Wasser- und Feuerschäden sowie Brandbekämpfung), zu Stromausfällen, Einbrüchen und Erste Hilfe. Zusätzlich sind die Feuerwehren in Uster und Aathal-Seegräben mit der Brandbekämpfung in Archivräumen instruiert.

Bei beschädigten oder kontaminierten Akten wird vor der Einlagerung eine Triage durchgeführt. Bei Kontaminationen oder Beschädigungen arbeitet archivsuisse mit der auf Wiederherstellung von Archivgut spezialisierten Firma DocuSave zusammen.

Infrastrukturelle, IT-technischen und organisatorische Vorkehrungen sind in den Abschnitten Archivräume und IT erwähnt.

Archivsuisse unterhält im Rahmen der Managementprozesse auch regelmässige Risikobeurteilungen.