

## colada Security Statement

Wir von salce stellen sicher, dass Daten und Informationen, die in colada verarbeitet werden zu jedem Zeitpunkt sicher sind. Sicherheit hat bei salce einen sehr hohen Stellenwert, weshalb wir ein ausgeklügeltes, "state-of-the-art" Sicherheitskonzept auf allen Stufen einsetzen. Bei der Arbeit mit colada können Sie darauf vertrauen, dass wir alles daran setzen um Ihr und unser Kapital zu schützen.

Die Eckpfeiler unseres Sicherheitskonzeptes sind:

- Hochqualifizierte Mitarbeiter mit langjähriger Erfahrung im Security, Database und Application-Umfeld
- Laufende Weiterentwicklung und Erweiterung des Sicherheitskonzeptes
- Grösstmögliche Redundanz aller eingesetzten Systeme

## Sicherheit auf allen Stufen:

### salce corporate security

#### Physische Sicherheit

Unsere Entwicklungs-Umgebung ist an unserem Hauptsitz in Schaffhausen (Schweiz) untergebracht. An diesem Standort haben wir alle erdenklichen Sicherheitsmassnahmen für Mitarbeiter und Technik realisiert. Diese Systeme werden laufend überprüft und optimiert. Dieser Schutz umfasst:

- Schutz vor Hochwasser und Feuer
- Schutz vor fremdem Zugriff
- Schutz vor Stromunterbrüchen und Spannungsschwankungen
- Sicherstellung der Verbindung ins Internet

#### Interne Sicherheit

Unsere Entwicklungsumgebung umfasst Firewalls, Intrusion Detection Systeme, SSL-Verschlüsselung und andere, durch uns selbst entwickelte Sicherheit-Mechanismen.

### Sichere Rechenzentren

#### Zusammenarbeit mit zertifizierten Rechenzentren

Durch die Zusammenarbeit mit zertifizierten Rechenzentren bieten wir ein Höchstmass an Service-Qualität und Verfügbarkeit.

#### Datensicherheit / Backup

Ihre Daten sind bei uns sicher. Sollten Sie doch einmal Ihre Daten verlieren oder löschen, so haben wir mit unserem Backup und Recovery-System vorgesorgt. Unser transaktionsbasiertes Datenbanksystem ermöglicht uns jede Aktion des aktuellen Tages rückgängig zu machen.

### **Application Security**

Das ausgeklügelte Datenmodell von colada stellt sicher, dass jeder Kunde nur seine eigenen Daten und nicht auch die Daten anderer Kunden einsehen kann. Dieses Modell wird während der gesamten Dauer einer Session mit jeder Server-Anfrage neu überprüft. Zusätzlich hat jeder Kunde seine eigene, physisch getrennte Datenbank.

### **OS Security / Antivirus**

Unsere Hardware befindet sich zu jedem Zeitpunkt auf dem vom Hersteller empfohlenen Patchlevel. Zusätzlich sorgen Antiviren-, IDS und externe Überwachungsprogramme für einen umfassenden Schutz.

### **Database Security**

Der Zugriff auf die Datenbank in colada findet immer über das Framework statt und ist auf eine möglichst geringe Zahl von Access-Points limitiert. Entwicklungs- und Produktiv-Systeme sind vollkommen voneinander getrennt und haben auch keine gemeinsame Passwort-Datenbank.

## **Internet-Sicherheit**

### **Datentransport via SSL**

Wann immer möglich und sinnvoll wird der Datenverkehr vollständig SSL-verschlüsselt.

### **Data Encryption**

Unabhängig von allen Standard-Verschlüsselungen werden die colada-Daten noch zusätzlich durch eine eigene, proprietäre Verschlüsselung gesichert.

### **Netzwerk Sicherheit**

Durch die redundante Anbindung an nationale und internationale Internet Service Provider garantieren wir eine hohe Verfügbarkeit und kurze Zugriffszeiten

### **Firewalls**

Alle Server befinden sich hinter Firewalls, die den höchsten Ansprüchen genügen. Zusätzlich wird jeder Zugriff auf unsere Systeme von einem Intrusion-Detection-System überwacht und auffällige Datenpakete automatisch abgeblockt

## **Anwender-Sicherheit**

### **User Authentication**

Jeder colada Anwender muss sich in colada authentifizieren. Dies findet in der Regel über Name und Passwort statt. Ein User kann sich nicht mehrmals im System einloggen.

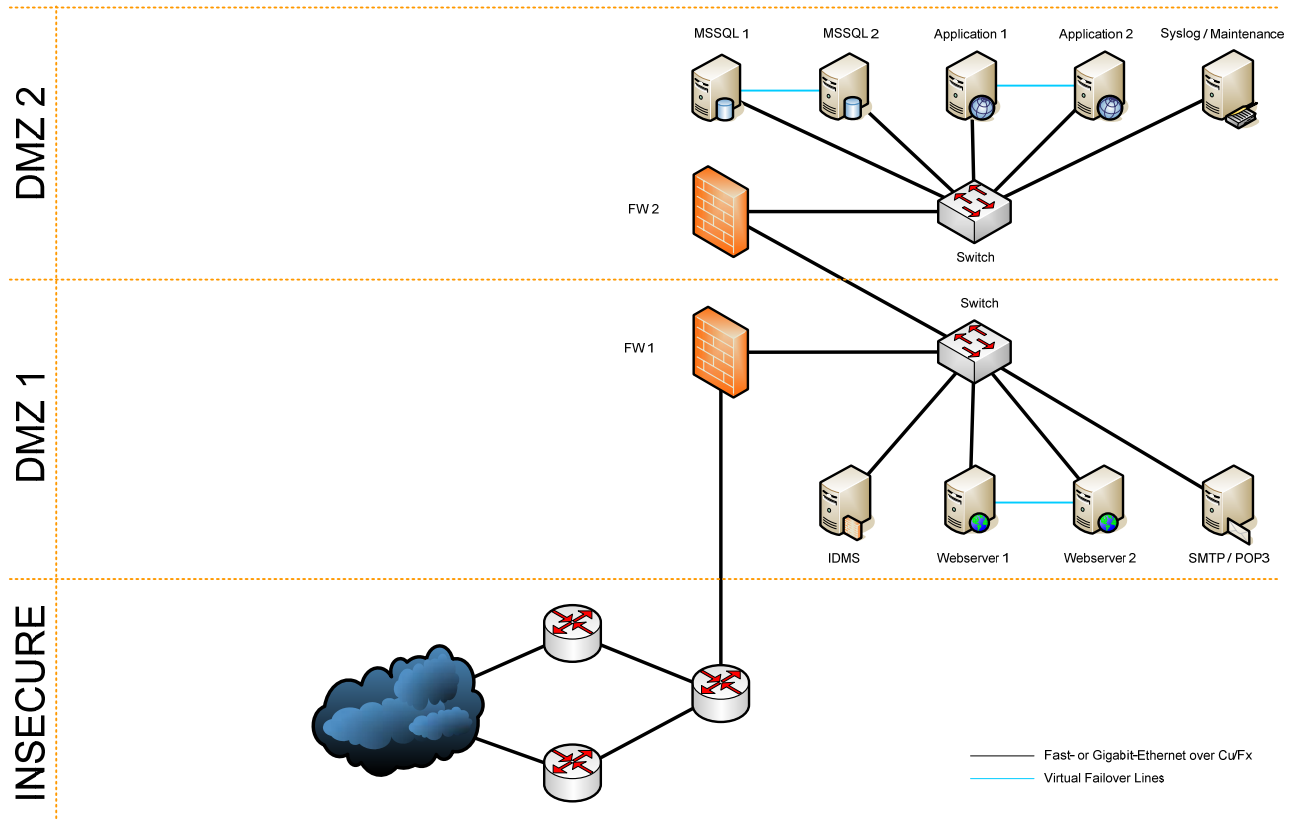
### **Strong Authentication**

Optional kann der Zugriff auf colada zusätzlich durch ein Strong-Authentication-System gesichert werden, das die Zugriffssicherheit über periodisch generierte Tokens als zusätzliches Authentifizierungsmerkmal erhöht.

### **Kundendaten**

Alle Daten, die in colada eingegeben und verarbeitet werden gehören vollumfänglich dem jeweiligen Kunden.

## colada Infrastruktur



Die colada Infrastruktur wird in einem zweistufigen Sicherheitssystem betrieben. Dadurch kann eine vollständige Trennung der Datenbank- und Applikationsserver vom unsicheren, öffentlichen Internet gewährleistet werden. Restriktive Zugriffsregeln sorgen dafür dass nur autorisierten Systemen der Zugriff gewährt wird. Die Remote-Verwaltung der in DMZ 1 platzierten Systeme kann nur von Systemen die über das entsprechende Zertifikat, sowie Benutzern mit gültigem Zertifikat und Passwort erfolgen. DMZ 2 Systeme können nur lokal gewartet werden.

## salce + partner ag Service Level Agreement

### 1. Service Class

Die Services Classes beschreiben die zeitliche Verfügbarkeit der Hotline und die maximale Zeit zur Wiederherstellung des Betriebszustandes.

Service Class	Wiederherstellung des Betriebszustandes	Verfügbarkeit
8/5x10 (Standart)	8 Stunden	99.5%
7x24 (Optional)	4 Stunden	99.9%

### 2. Verfügbarkeit

salce + partner ag garantiert dem Kunden 99,5% (resp. 99.9%) Verfügbarkeit der vertraglich abgemachten Services.

Nicht unter diese Garantie fallen:

Wartung, nach erfolgter Benachrichtigung  
Ausfälle von Leitungen und Systemen die nicht unter Kontrolle von salce + partner ag stehen  
Ausfall von Leitungen und Geräten die beim Kunden platziert sind oder vom Kunden gewartet werden  
Ausfälle die von höherer Natur ausgelöst werden

Abgesicherte Ereignisse

Das Network Operating Center (NOC) von salce + partner ag ist gegen folgende Ereignisse abgesichert:

Schutz gegen Stromausfall  
Schutz gegen Hochwasser  
Schutz gegen Datenverlust  
Schutz gegen Fehler von Hard- und Software  
Schutz gegen Feuer  
Sicherstellung der Connectivity

Um die Sicherheit und Verfügbarkeit zu erhöhen, werden folgende pro-aktive Massnahmen eingesetzt:

Tägliches Backup der Betriebssysteme, Applikationen und Daten auf Magnetband  
SQL Dump auf Harddisk, zur Wiederherstellung von Datenbankinkonsistenzen  
Real-Time Monitoring mit Benachrichtigung  
Redundante Auslegung der Infrastruktur (In Vorbereitung, redundanter Standort im Raum Zürich)  
Firewall und Host basierte Intrusion Detection  
Anti-Virus Software mit täglichem Update

Ein Ausfall definiert sich durch den Umstand, dass der Kunde den gebotenen Service nicht oder nur unter starker Verzögerung (Latenz > 30s) in Anspruch nehmen kann.

### 3. Hotline

Den salce + partner ag SLA-Kunden steht während den definierten Reaktionszeiten eine spezielle Hotline zur Verfügung. Diese bietet Gewähr dafür, dass das Anliegen direkt zu den Kontaktpersonen geleitet und unnötige Wartezeit vermieden wird. Bei einer Störungsmeldung erhält der Kunde eine Referenz-Nummer (Ticket), die als Referenz für die gesamte Abwicklung des Störfalles dient. Für Probleme die über keine Referenz-Nummer verfügen, treten die Bestimmungen des SLA nicht in Kraft.

#### **4. Kundenbenachrichtigung**

salce + partner ag verpflichtet sich die Termine für Wartungsarbeiten, soweit als möglich 48 Stunden im Voraus, dem Kunden mitzuteilen. salce + partner ag ist bemüht das Wartungsfenster auf Samstag/Sonntag ab 22:00 Uhr zu legen. Bei Kurzfristigen Ereignissen (z.B. Viren, Patches, Angriffen) kann die Wartung auch an Werktagen durchgeführt werden. Bei einem Problem wird der Kunde innerhalb von 45 Minuten über den Unterbruch und deren Folgen informiert. Die Kundenbenachrichtigung erfolgt über einen im Voraus festgelegten Kommunikationskanal.

#### **5. Wartung**

Um die Servicequalität zu gewährleisten wird pro Quartal eine regelmässige Wartung durchgeführt. Falls es die Betriebssicherheit erfordert, werden pro-aktive Wartungsarbeiten durchgeführt. salce + partner ag ist bemüht die Unterbruchszeiten bei Wartungsarbeiten möglichst gering zu halten. Die Wartungsarbeiten werden dem Kunden mindestens 48 Stunden im Voraus mitgeteilt.

#### **6. Reaktionszeiten**

Die Reaktionszeit bei aufgetretenen Problemen beträgt maximal 45 Minuten. Die Wiederherstellung erfolgt gemäss der Definition in der gewählten Service Class.

#### **7. Gültigkeit**

Das SLA ist nur für die im Vertrag aufgeführten Services und die Vertragslaufzeit gültig. Dieses SLA ist nur in Verbindung mit einem Hosting/Maintenance Vertrag gültig.