

Technische und organisatorische Maßnahmen

Cloud-Anwendungen für die Zutrittskontrolle

1. GELTUNGSBEREICH

Die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen gelten für die Cloud-Plattformen von Salto zur Zutrittskontrolle, auf die in der entsprechenden Datenverarbeitungsvereinbarung Bezug genommen wird.

Salto behält sich das Recht vor, diese Maßnahmen jederzeit ohne Vorankündigung zu ändern und zu aktualisieren, solange wir ein vergleichbares oder besseres Sicherheitsniveau aufrechterhalten.

2. LISTE DER TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN

Nachfolgend finden Sie die Liste der von Salto angewandten Sicherheitsmaßnahmen:

- › Sicherheitsrichtlinien: Salto implementiert Sicherheitsrichtlinien und -standards, die im gesamten Unternehmen verbindlich sind. Sicherheitsrichtlinien werden regelmäßig überprüft und bei Bedarf aktualisiert, um das Risiko zu mindern und Plattformen und Daten sicher zu halten.
- › Security Awareness: Salto führt regelmäßig Sensibilisierungskampagnen im gesamten Unternehmen durch, um die Risiken der Benutzer zu vermeiden und zu mindern.
- › Physische Sicherheit: Salto schützt seine Einrichtungen mit geeigneten Zutrittskontrollen (z. B. intelligenten Türschlössern), um den Zutritt auf befugtes Personal zu beschränken. Darüber hinaus verfügen sichere Bereiche wie Rechenzentren über zusätzliche Schutzmaßnahmen gegen Umweltgefahren. Um die ordnungsgemäße Funktionalität zu gewährleisten, werden Schutzmaßnahmen (Klimaanlage, Feuerlöscher usw.) regelmäßig gewartet. Darüber hinaus arbeitet Salto mit vertrauenswürdigen Drittanbietern für Colocation zusammen, die ebenfalls physische Sicherheitskontrollen gemäß den Industriestandards durchführen.
- › Sicherheitsvorfälle: Salto unterhält Pläne zur Reaktion auf Vorfälle, einschließlich des Managements von Verletzungen des Schutzes personenbezogener Daten.
- › Zugriffskontrolle: Salto implementiert eine angemessene Zugriffskontrolle, um sicherzustellen, dass der Zugriff auf die Anwendungen und Systeme im Allgemeinen gemäß den Grundsätzen des geringsten Privilegs und des Wissensbedarfs eingeschränkt ist. Alle Mitarbeiter greifen mit einer eindeutigen Kennung (Benutzer-ID) auf die Systeme von Salto zu. Im Falle eines Ausscheidens des Personals aus dem Unternehmen werden seine Zugriffsrechte widerrufen.
- › Netzwerksicherheit: Salto verwendet verschlüsselte und authentifizierte Verbindungen für die Verbindung zu Plattformen und Systemen im Allgemeinen, indem Sicherheitsfunktionen wie Firewalls, VPNs, Authentifizierungsmechanismen usw. verwendet werden.
- › Sichere Arbeitsplätze: Salto implementiert angemessenen Schutz für die Geräte des Endbenutzers, wie z. B. erweiterten Malware-Schutz, Festplattenverschlüsselung und geeignete Patch-Levels.

- › **Datenschutz und Sicherheit by Design:** Salto wendet Datenschutz und Sicherheit durch Designprinzipien an, wenn ein neues System eingeführt oder ein bestehendes verbessert wird.
- › **Schwachstellenmanagement:** Salto führt regelmäßig Sicherheitsüberprüfungen durch und behebt die identifizierten Schwachstellen, um die Plattformen sicher zu halten.
- › **Ausfallsicherheit:** Salto unterhält Backup- und Disaster Recovery-Pläne für Notfälle.
- › **Salto führt regelmäßige Überprüfungen durch, um die Einhaltung der Sicherheitsrichtlinien und -standards sicherzustellen.**

Disclaimer:

This is a downloadable version of the website content that we make available to you for informative purposes for an easier consultation and filling. However, SALTO assumes no responsibility for any errors or typos that the downloadable version may contain.

As SALTO reserves the right to modify this content from time to time, please check on the Legal section of our website to find the latest version of the legal documents and their updates.