Misure tecniche e organizzative

Applicazioni cloud di controllo accessi

1. CAMPO DI APPLICAZIONE

Le misure tecniche e organizzative descritte di seguito si applicano alle piattaforme cloud di controllo degli accessi di Salto che fanno riferimento a queste misure tecniche e organizzative nel relativo accordo sul trattamento dei dati applicabile.

Salto si riserva il diritto di modificare e aggiornare queste misure in qualsiasi momento senza preavviso, purché si mantenga un livello di sicurezza comparabile o migliore.

2. ELENCO DELLE MISURE TECNICHE E ORGANIZZATIVE

Di seguito puoi trovare l'elenco delle misure di sicurezza applicate da Salto:

- Politica di sicurezza: Salto implementa politiche e standard di sicurezza obbligatori in tutta l'organizzazione. Le politiche di sicurezza vengono riviste periodicamente e aggiornate se necessario per mitigare l'esposizione al rischio e mantenere le piattaforme e i dati protetti.
- Consapevolezza della sicurezza: Salto conduce regolarmente campagne di sensibilizzazione in tutta l'organizzazione per prevenire e mitigare i rischi degli utenti.
- Sicurezza fisica: Salto protegge le proprie strutture utilizzando adeguati sistemi di controllo degli accessi (es. serrature intelligenti) per limitare l'accesso al personale autorizzato. Inoltre, le aree sicure come i data center dispongono di misure di protezione aggiuntive contro le minacce ambientali. Per salvaguardare il corretto funzionamento, le misure di protezione (climatizzazione, estinzione incendi, ecc.) sono soggette a regolare manutenzione. Inoltre, Salto si avvale di fornitori di colocation di terze parti di fiducia che incorporano anche controlli di sicurezza fisica in conformità con gli standard del settore.
- Incidenti di sicurezza: Salto mantiene piani di risposta agli incidenti, inclusa la gestione delle violazioni dei dati personali.
- Controllo degli accessi: Salto implementa un controllo degli accessi appropriato per garantire che l'accesso alle applicazioni e ai sistemi in generale sia limitato in base al privilegio minimo e alla necessità di conoscere i principi. Tutto il personale accede ai sistemi Salto con un identificatore univoco (ID utente). Nel caso in cui il personale lasci l'azienda, i suoi diritti di accesso vengono revocati.
- Sicurezza della rete: Salto utilizza connessioni crittografate e autenticate per la connessione a piattaforme e sistemi in generale utilizzando funzionalità di sicurezza come firewall, VPN, meccanismi di autenticazione, ecc.
- Postazioni di lavoro sicure: Salto implementa una protezione adeguata sui dispositivi dell'utente finale, come protezione antimalware avanzata, crittografia del disco rigido e livelli di patch appropriati.
- Privacy e sicurezza in base alla progettazione: Salto applica i principi di privacy e sicurezza in base alla progettazione quando adotta un nuovo sistema o ne migliora uno esistente.
- Gestione delle vulnerabilità: Salto effettua revisioni di sicurezza su base periodica e corregge le vulnerabilità identificate al fine di mantenere le piattaforme sicure.
- Resilienza: Salto adotta piani di backup e ripristino di emergenza per situazioni avverse.

Copyright ©2025 SALTO Systems S.L. All rights reserved

- **Garanzia: Salto conduce revisioni periodiche per garantire la conformità con le politiche e gli standard di sicurezza.**

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.

Copyright ©2025 SALTO Systems S.L. All rights reserved