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 reserves the right to modify and update these measures at any time without notice as long as we maintain a comparable or better level of security.

2. ELENCO DELLE MISURE TECNICHE E ORGANIZZATIVE

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

- Politiche 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 accesso: SALTO implements appropriate access control to ensure access to the applications and systems in general is restricted according to least privilege and need to know principles. All personnel access SALTO's systems with a unique identifier (user ID). In case personnel leaves the company, their access rights are revoked.
- 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.

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

Disclaimer: