Tekniska och organisatoriska åtgärder

Molnapplikationer för kontrollenhet

1. OMFATTNING

De tekniska och organisatoriska åtgärder som beskrivs nedan gäller för Salto:s molnplattformar för åtkomstkontroll som hänvisas till dessa tekniska och organisatoriska åtgärder i dess tillämpliga databearbetningsavtal.

Salto förbehåller sig rätten att när som helst ändra och uppdatera dessa åtgärder utan föregående meddelande, så länge vi upprätthåller en jämförbar eller bättre säkerhetsnivå.

2. FÖRTECKNING ÖVER TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER

Nedan hittar du listan över säkerhetsåtgärder som tillämpas av Salto:

- Säkerhetspolicyer: Salto implementerar säkerhetspolicyer och standarder som är obligatoriska i hela organisationen. Säkerhetspolicyer granskas regelbundet och uppdateras vid behov för att minska riskexponeringen och hålla plattformar och data säkra.
- Säkerhetsmedvetenhet: Salto genomför regelbundna informationskampanjer i hela organisationen för att förebygga och minska användarnas risker.
- Fysisk säkerhet: Salto skyddar sina anläggningar med hjälp av lämpliga passersystem (exempelvis smarta dörrlås) för att begränsa åtkomsten till behörig personal. Vidare har säkra områden som datacenter ytterligare skyddsåtgärder mot miljöhot. För att skydda korrekt funktionalitet genomgår skyddsåtgärder (luftkonditionering, brandutrotning osv.) regelbundet underhåll. Salto använder också betrodda tredjepartsleverantörer av samlokalisering som även införlivar fysiska säkerhetskontroller i enlighet med branschstandarder.
- Säkerhetsincidenter: Salto upprätthåller incidenthanteringsplaner inklusive hantering av personuppgiftsincidenter.
- Åtkomstkontroll: Salto implementerar lämplig åtkomstkontroll för att se till att åtkomsten till applikationer och system i allmänhet är begränsad enligt minsta privilegium och behöver känna till principerna. All personal har åtkomst till Salto:s system med en unik identifierare (användar-ID). Om personalen lämnar företaget återkallas deras åtkomsträttigheter.
- Salto använder krypterade och autentiserade anslutningar för att ansluta till plattformar och system i allmänhet genom att använda säkerhetsfunktioner som brandväggar, VPN, autentiseringsmekanismer, osv.
- Säkra arbetsstationer: Salto implementerar lämpligt skydd över slutanvändarens enheter, såsom avancerat skydd mot skadlig programvara, hårddiskkryptering och lämpliga patchnivåer.
- Integritet och säkerhet genom design: Salto tillämpar integritet och säkerhet genom designprinciper när man antar ett nytt system eller förbättrar ett redan befintligt.
- Sårbarhetshantering: Salto genomför regelbundet säkerhetsgranskningar och åtgärdar de identifierade sårbarheterna för att hålla plattformarna säkra.
- Motståndskraft: Salto antar planer för säkerhetskopiering och katastrofåterställning för ogynnsamma situationer.
- Försäkran: Salto genomför regelbundna granskningar för att säkerställa efterlevnad av säkerhetspolicyer och standarder.

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.