Tekniske og organisatoriske foranstaltninger

Cloud-applikationer til adgangskontrol

1. OMFANG

De tekniske og organisatoriske foranstaltninger, der er beskrevet nedenfor, gælder for Saltos cloud-platforme til adgangskontrol. Der henvises til disse tekniske og organisatoriske foranstaltninger i deres gældende databehandlingsaftale.

Salto forbeholder sig ret til at ændre og opdatere disse foranstaltninger når som helst uden varsel, så længe vi opretholder et tilsvarende eller bedre sikkerhedsniveau.

2. LISTE OVER TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER

Nedenfor finder du en liste over sikkerhedsforanstaltninger, der anvendes af Salto:

- Sikkerhedspolitikker: Salto implementerer sikkerhedspolitikker og -standarder, der er obligatoriske på tværs af organisationen. Sikkerhedspolitikker gennemgås regelmæssigt og opdateres efter behov for at mindske risikoeksponeringen og holde platforme og data sikre.
- Sikkerhedsbevidsthed: Salto gennemfører regelmæssige oplysningskampagner på tværs af organisationen for at forebygge og mindske brugernes risici.
- Fysisk sikkerhed: Salto beskytter sine faciliteter ved hjælp af passende adgangskontrolsystemer (f.eks. intelligente dørlåse) for at begrænse adgang til autoriseret personale. Derudover har sikrede områder som datacentre yderligere beskyttelsesforanstaltninger mod miljøtrusler. For at beskytte korrekt funktionalitet skal beskyttelsesforanstaltninger (klimaanlæg, brandsikring osv.) regelmæssigt vedligeholdes. Derudover bruger Salto betroede tredjeparts colocation-udbydere, som også inkorporerer fysiske sikkerhedskontroller i overensstemmelse med branchestandarder.
- Sikkerhedshændelser: Salto opretholder hændelsesresponsplaner, herunder håndtering af brud på datasikkerheden for personlige oplysninger.
- Adgangskontrol: Salto implementerer passende adgangskontrol for at sikre, at adgangen til applikationerne og systemerne generelt er begrænset i henhold til principperne for minimale privilegier og brug for kendskab. Alle medarbejdere tilgår Saltos systemer med en unik identifikator (bruger-id). Alle medarbejdere, der forlader virksomheden, får deres adgangsrettigheder tilbagekaldt.
- Netværkssikkerhed: Salto anvender krypterede og godkendte forbindelser til at oprette forbindelse til platforme og systemer generelt ved hjælp af sikkerhedsfunktioner såsom firewalls, VPN'er, godkendelsesmekanismer osv.
- Sikre arbejdsstationer: Salto implementerer passende beskyttelse af slutbrugerens enheder, såsom avanceret anti-malwarebeskyttelse, harddiskkryptering og passende patchniveauer.
- Databeskyttelse og sikkerhed via design: Salto inkluderer altid databeskyttelse og sikkerhed i deres designprincipper, når der implementeres et nyt system, eller et eksisterende system forbedres.
- Sårbarhedsstyring: Salto udfører regelmæssigt sikkerhedsvurderinger og afhjælper de identificerede sårbarheder for at holde platformene sikre.
- Modstandsdygtighed: Salto implementerer backup- og katastrofegenopretningsplaner i tilfælde af uønskede situationer.

- Sikring: Salto foretager regelmæssige gennemgange for at sikre overholdelse af sikkerhedspolitikker og -standarder.