

Tekniset ja organisatoriset toimenpiteet

Kulunvalvonnan pilvisovellukset

1. SOVELTAMISALA

Jäljempänä kuvattuja teknisiä ja organisatorisia toimenpiteitä sovelletaan Salton kulunvalvonnan pilvialustoihin, joihin viitataan näihin teknisiin ja organisatorisiin toimenpiteisiin sen sovellettavassa tietojenkäsittelysopimuksessa.

Salto pidättää oikeuden muuttaa ja päivittää näitä toimenpiteitä milloin tahansa ilman ennakoilmoitusta niin kauan kuin säilytämme vastaavan tai paremman turvallisuustason.

2. LUETTELO TEKNISISTÄ JA ORGANISATORISISTA TOIMENPITEISTÄ

Alla on luettelo Salton soveltamista turvatoimista:

- **Turvallisuuskäytännöt:** Saltolla on koko organisaatiossa käytössä pakolliset turvallisuuskäytännöt ja -standardit. Turvallisuuskäytäntöjä tarkistetaan säännöllisesti ja päivitetään tarvittaessa riskien vähentämiseksi sekä alustojen ja tietojen turvallisuuden ylläpitämiseksi.
- **Turvallisuustietoisuus:** Salto toteuttaa säännöllisesti organisaatiossaan tietoisuuskampanjoita käyttäjiin liittyvien riskien estämiseksi ja pienentämiseksi.
- **Fyysinen turvallisuus:** Salto suojaa tilojaan asianmukaisilla kulunvalvontajärjestelmillä (esimerkiksi älylukoilla), joilla pääsy rajoitetaan valtuutettuun henkilöstöön. Lisäksi suojatuilla alueilla, kuten datakeskuksissa, on käytössä lisäsuojatoimenpiteitä ympäristöuhkia vastaan. Suojausmekanismit (ilmastointi, palonsammutus jne.) huolletaan säännöllisesti, jotta ne toimisivat moitteettomasti. Lisäksi Salto käyttää luotettavia kolmannen osapuolen konesalipalveluntarjoajia, joilla on myös käytössä alan normien mukaiset fyysiset turvatoimet.
- **Turvallisuuspoikkeamat:** Salto ylläpitää suunnitelmia poikkeamiin reagoimisen varalta, mukaan lukien henkilötietojen tietoturvaloukkausten hallinta.
- **Kulunvalvonta:** Salto toteuttaa asianmukaisen kulunvalvonnan varmistaakseen, että pääsyä sovelluksiin ja järjestelmiin yleensä rajoitetaan pienimmän etuoikeuden ja tarpeellisuusperiaatteiden mukaisesti. Kaikki työntekijät käyttävät Salton järjestelmiä yksilöllisellä tunnisteella (käyttäjätunnus). Jos henkilöstö lähtee yrityksestä, hänen käyttöoikeutensa peruutetaan.
- **Verkon turvallisuus:** Salto käyttää salattuja ja todennettuja yhteyksiä alustoihin ja järjestelmiin liittymiseksi yleensä käyttämällä tietoturvaominaisuuksia, kuten palomuureja, VPN-verkkoja, todennusmekanismeja jne.
- **Turvalliset työasemat:** Salto käyttää loppukäyttäjän laitteissa asianmukaista suojausta, kuten edistyksellistä haittaohjelasuojausta, kiintolevyn salausta ja asianmukaisia korjaustasoja.
- **Sisäänrakennetun yksityisyydensuojan ja turvallisuuden periaate:** Salto soveltaa sisäänrakennetun yksityisyydensuojan ja turvallisuuden periaatetta, kun se ottaa käyttöön uuden järjestelmän tai parantaa olemassa olevaa järjestelmää.
- **Haavoittuvuuksien hallinta:** Salto tekee tietoturvatarkastuksia säännöllisesti ja korjaa havaitut haavoittuvuudet, jotta alustat pysyvät turvallisina.
- **Häiriönsietokyky:** Salto käyttää varmuuskopiointia ja palautumissuunnitelmia epäsuotuisia tilanteita varten.

- **Varmistus:** Salto tekee säännöllisiä tarkastuksia varmistaakseen, että tietoturvakäytäntöjä ja -standardeja noudatetaan.

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.