Mesures techniques et organisationnelles

Applications de contrôle d’accès Cloud

1. PORTÉE

Les mesures techniques et organisationnelles décrites ci-dessous s'appliquent aux plates-formes cloud de contrôle d'accès de SALTO auxquelles il est fait référence à ces mesures techniques et organisationnelles dans son accord de traitement de données applicable.

SALTO se réserve le droit de modifier et de mettre à jour ces mesures à tout moment et sans préavis tant que nous maintenons un niveau de sécurité comparable ou supérieur.

2. LISTE DES MESURES TECHNIQUES ET ORGANISATIONNELLES

Vous trouverez ci-dessous la liste des mesures de sécurité appliquées par SALTO:

- Politiques de sécurité: SALTO met en œuvre des politiques et des normes de sécurité qui sont obligatoires dans toute l'organisation. Les politiques de sécurité sont revues périodiquement et mises à jour si nécessaire pour atténuer l'exposition aux risques et maintenir la sécurité des plateformes et des données.
- Sensibilisation à la sécurité: SALTO mène des campagnes de sensibilisation régulières dans toute l'organisation pour prévenir et atténuer les risques des utilisateurs.
- Sécurité physique: SALTO protège ses installations en utilisant des systèmes de contrôle d'accès appropriés (par exemple, des serrures de porte intelligentes) pour limiter l'accès au personnel autorisé. De plus, les zones sécurisées telles que les centres de données disposent de mesures de protection supplémentaires contre les menaces environnementales. Afin de préserver leur bon fonctionnement, les mesures de protection (climatisation, extinction d'incendie, etc.) font l'objet d'un entretien régulier. En outre, SALTO utilise des fournisseurs de colocation tiers de confiance qui intègrent également des contrôles de sécurité physique conformes aux normes de l'industrie.
- Incidents de sécurité: SALTO maintient des plans de réponse aux incidents, y compris la gestion des violations de données personnelles.
- Contrôle d’accès: SALTO met en œuvre un contrôle d'accès approprié pour garantir que l'accès aux applications et aux systèmes en général est limité selon les principes du moindre privilège et du besoin de connaître. Tout le personnel accède aux systèmes de SALTO avec un identifiant unique (ID utilisateur). En cas de départ du personnel de l'entreprise, ses droits d'accès sont révoqués.
- Sécurité Internet: SALTO utilise des connexions cryptées et authentifiées pour se connecter aux plates-formes et aux systèmes en général en utilisant des capacités de sécurité telles que des pare-feu, des VPN, des mécanismes d'authentification, etc.
- Postes de travail sécurisés: SALTO met en œuvre une protection appropriée sur les appareils de l'utilisateur final, telle qu'une protection antimalware avancée, un chiffrement du disque dur et des niveaux de correctifs appropriés.
- Confidentialité et sécurité dès la conception: SALTO applique les principes de confidentialité et de sécurité dès la conception lors de l'adoption d'un nouveau système ou de l'amélioration d'un système existant.

- Gestion des vulnérabilités: SALTO effectue périodiquement des revues de sécurité et corrige les vulnérabilités identifiées afin de maintenir la sécurité des plateformes.
- Élasticité: SALTO adopte des plans de sauvegarde et de reprise après sinistre pour les situations défavorables.
- Assurance: SALTO procède à des examens réguliers pour garantir la conformité aux politiques et normes de sécurité.