Medidas Técnicas e Organizacionais

Aplicativos de nuvem de controle de acesso

1. ÂMBITO

As medidas técnicas e organizacionais descritas abaixo aplicam-se às plataformas de cloud de controle de acesso da SALTO que são referidas a essas medidas técnicas e organizacionais em seu contrato de processamento de dados aplicável.

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. LISTA DE MEDIDAS TÉCNICAS E ORGANIZACIONAIS

Abaixo você encontra a lista de medidas de segurança aplicadas pela SALTO:

- Políticas de segurança: A SALTO implementa políticas e padrões de segurança que são obrigatórios em toda a organização. As políticas de segurança são revisadas periodicamente e atualizadas, se necessário, para mitigar a exposição ao risco e manter as plataformas e os dados seguros.
- Conscientização sobre segurança: A SALTO realiza campanhas regulares de conscientização em toda a organização para prevenir e mitigar os riscos dos usuários.
- Segurança física: A SALTO protege as suas instalações utilizando sistemas de controlo de acesso adequados (por exemplo, fechaduras inteligentes) para restringir o acesso ao pessoal autorizado. Além disso, áreas seguras, como data centers, possuem medidas de proteção adicionais contra ameaças ambientais. Para proteger a funcionalidade adequada, as medidas de proteção (ar condicionado, extinção de incêndio etc.) passam por manutenção regularmente. Além disso, a SALTO usa provedores de colocation terceirizados confiáveis que também incorporam controles de segurança física em conformidade com os padrões do setor.
- Incidentes de segurança: A SALTO mantém planos de resposta a incidentes, incluindo gerenciamento de violação de dados pessoais.
- Controlo de acessos: 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.
- Segurança de rede: A SALTO emprega conexões criptografadas e autenticadas para conexão com plataformas e sistemas em geral usando recursos de segurança como firewalls, VPNs, mecanismos de autenticação, etc.
- Estações de trabalho seguras: O SALTO implementa proteção adequada nos dispositivos do usuário final, como proteção antimalware avançada, criptografia de disco rígido e níveis de patch apropriados.
- Privacidade e segurança por design: A SALTO aplica princípios de privacidade e segurança por design ao adotar um novo sistema ou aprimorar um existente.
- Gerenciamento de vulnerabilidades: A SALTO realiza revisões de segurança periodicamente e corrige as vulnerabilidades identificadas para manter as plataformas seguras.

- Resiliência: A SALTO adota planos de backup e recuperação de desastres para situações adversas.
- Garantia: A SALTO realiza revisões regulares para garantir o cumprimento das políticas e normas de segurança.

Isenção de responsabilidade: