技术和组织措施

访问控制云应用

1.范围

以下描述的技术和组织措施适用于 SALTO 的访问控制云平台，在其适用的数据处理协议中提及这些技术和组织措施。

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. 技术和组织措施清单

您可以在下面找到 SALTO 应用的安全措施列表：

- 安全政策： SALTO 实施整个组织强制执行的安全策略和标准。安全策略会定期审查并在需要时进行更新，以减轻风险暴露并维护平台和数据的安全。
- 安全意识：SALTO 在整个组织内定期开展宣传活动，以预防和减轻用户的风险。
- 物理安全： SALTO 使用适当的访问控制系统（例如智能门锁）保护其设施，以限制授权人员的访问。此外，数据中心等安全区域还有针对环境威胁的额外保护措施。为保护正常功能，保护措施（空调、灭火等）会定期进行维护。此外，SALTO 使用受信任的第三方托管服务提供商，这些托管服务提供商还结合了符合行业标准的物理安全控制。
- 安全事件：SALTO 维护包括个人数据泄露管理在内的事件响应计划。
- 门禁控制: 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.
- 网络安全：SALTO 采用加密和经过身份验证的连接，通过使用防火墙、VPN、身份验证机制等安全功能来连接到平台和系统。
- 安全工作站：SALTO 对最终用户的设备实施适当的保护，例如高级反恶意软件保护、硬盘加密和适当的补丁级别。
- 隐私和安全设计： 在采用新系统或增强现有系统时，SALTO 通过设计原则应用隐私和安全性。
- 漏洞管理：SALTO 定期进行安全审查并修复已识别的漏洞，以维护平台安全。
- 弹性：SALTO针对不利情况采取备份和灾难恢复计划。
- 保证： SALTO 进行定期审查，以确保符合安全政策和标准。

version of the legal documents and their updates.