SaaS 应用的安全防护措施

SaaS 平台的安全能力并不等同于 SaaS 应用的安全能力，SaaS 产品/服务自身还需具备足够的安全保障能力。以 iLabPower 创新云社区为例，SaaS 产品须具备网络级、数据库系统级、环境级、职员级、操作系统级等全面的网络环境安全保证。具体措施如下：

（1） 用户访问

✧ 访问接口安全

- 采用更安全的 https 协议（基于 SSL 传输加密协议）
- URL 经过算法加密
- 请求携带的重要参数会进行加密并且拥有过期属性

✧ 权限安全

- 登陆密码经过加密算法，每个账号与终端绑定
- UC 产品授权限制
- 基于员工业务系统角色进行授权和访问
- 权限精细化控制并且基于最小化权限原则

✧ 访问控制

- 员工有唯一账号，账号有效性和在职转态进行绑定，离职员工账号无法使用
- 账户登录密码错误保护机制，登录日志实时保存以供审计
- 审计：信息系统的日志和权限审核记录通过备份方式保存，以供需要时调取审计

✧ 数据安全

- 读写分离，保障数据完整性与正常运行，降低因为宕机带来的影响
- 高可用系统中的两台服务器热备
- 将数据库做成分布数据库，分担每台服务器资源承受瓶颈
- 轻量级分布式文件系统，解决大容量存储和负载均衡问题
- 采用 IIS10，系统升级不会影响客户访问系统
- 定期安排系统和数据库巡检、数据备份和防路径篡改

- 现有网络结构提供的有效方法，扩展服务器带宽、吞吐量、处理能力，提高灵活性和可用性
- 定期进行数据灾备演练，模拟数据故障场景，增强数据灾难环境下的处置效率
- 数据的运维通过数据库管理软件进行鉴权、审批、操作日志留存审计，有效保障数据的安全

（2） 系统安全

✧ 组织安全

创新云社区团队由设计安全团队、研发安全团队、维护安全团队组成。

✧ 人员安全

员工行为符合所有法律、政策、流程以及创新云社区商业行为准则的要求；员工有履行其职责必备的知识、技能和经验。

✧ 交付安全

从设计、技术部署、支持及维护的产品全生命周期的安全防护，服务交付与公司核心流程紧密关联。

✧ 系统开发与维护

由研发和维护团队共同负责,服务于创新云社区的系统底层架构、业务逻辑实现以及上线的维护；定期进行漏洞扫描，补丁修复，协同为创新云社区客户打造安全的云服务环境。

✧ 研发流程与标准安全

强健的研发流程对于生产高质量和安全的产品很重要，创新云社区团队将产品安全基线纳入需求列表，并对客户使用场景进行威胁分析，从而实现产品的安全设计、安全开发。

✧ 灾难恢复/业务连续性

为了减少由硬件故障、自然灾害或者是其他的灾难带来的服务中断,创新云社区提供所有数据的灾难恢复计划，包括降低任何单个节点失效风险的多个组件：高可用性、数据保护、灾难恢复。

如果想了解更多，欢迎来电咨询

电话：010-82676188

邮箱：market@neotrident.com 官网：www.neotrident.com