上上签电子签约云平台
安全白皮书

版本：V6.0

发布时间：2025 年 4 月

目录

【声明】

本文档仅作为用户了解上上签信息安全保障体系的参考指引。对于本文档内容的准确性与适用性不作任何明示或暗示的保证。

由于产品或服务的迭代、升级或其他原因，本文档内容不定期进行更新，恕不另行通知。上上签保留对文档内容进行修改的权利。请从上上签官网获取本文档的最新版本。

1 前言

网络安全与隐私保护是上上签重要战略之一。我们基于先进的国际信息安全框架，构建技术防护与标准遵从保障体系。本白皮书旨在介绍电子签约云平台在组织架构、技术实现、合规运营及业务连续性等方面的策略与控制措施。

2 安全组织和人员

2.1 安全组织

信息安全委员会作为最高信息安全管理机构，决策和审批公司的总体信息安全战略；职责范围主要包括网络安全与隐私保护、数据治理、商密保护等。

上上签安全团队由一批经验丰富的网络安全、应用安全、数据安全、系统安全、隐私保护等方面的专家组成。工作职能包括建设及维护信息安全管理体系、监控与维护数字基础设施、安全开发流程审查、产品设计安全评估、漏洞与事件管理、提供安全意识培训和建议、处理面向客户的安全问题等。

2.2 人员安全

2.2.1 背景调查

员工入职背景调查的内容涵盖学历背景、工作经历、职业资格、犯罪记录等方面。在法律法规允许的情况下，还可能增加信用记录、专业成果验证、同行评价等，调查方式和具体程度取决于应聘人员的职位。

2.2.2 保密协议

全员签署劳动合同和保密协议，明确员工在履行职责中知悉的个人信息与商业秘密等数据有保密责任且不因雇用合同终止而结束。

2.2.3 安全培训

为员工持续提供安全培训是信息安全计划的重要组成部分，贯穿员工就职期间。安全培训和宣导的形式及内容，包括但不限于：

- 入职期间，新员工参加“新员工安全意识培训”项目，培训内容包括网络安全知识、信息安全行为守则和违规问责等。
- 设计创意海报文案宣传安全意识和信息安全行为守则，制作《安全小报》等并通过邮件传达至全员等。
- 举办年度信息安全活动周，互动式宣传最新安全资讯及热点案例等，并举行全员安全意识培训和考核。

- 根据职位与角色，员工可能要接受与安全领域相关的额外培训。例如：网络安全技能、安全编码实践、安全工具使用等专业知识。

2.2.4 离岗审查

按照调动、离职流程，对内部调离、离职人员进行离岗安全审查，包括离岗数据权限的清理或修改等。

3 安全合规与隐私保护

上上签致力于推动有效地遵守适用的法律和法规要求，保护用户数据的安全性和隐私性，并将安全合规与标准遵从融入产品设计与日常运营中，不断提升网络安全防护能力和数据安全保障水平，维护与客户的可信任关系。

3.1 安全合规

上上签基于 ISO/IEC 27001 国际标准构建企业风险管理框架，并扩展到数据治理。截至目前，通过的标准认证或安全测评如下表所示：

资质		测评/颁证机构	简介
国际标准	ISO/IEC 27001 信息安全管理体系	BSI（英国标准协会）	ISO/IEC 27001 全球企业广泛采用的信息安全管理标准，以风险管理为核心理念来管理公司和客户信息，并通过定期评估风险与控制措施来确保组织持续满足认证范围的要素及标准要求。
	ISO/IEC 27018 公有云个人信息保护管理体系	BSI（英国标准协会）	ISO/IEC 27018 专注于保护公共云中个人信息的国际标准，为云服务提供商提供一套隐私保护的控制措施和实务守则，旨在防止数据泄露、滥用或未经授权的访问，同时满足全球数据隐私保护法律法规的要求。
	ISO 22301 业务连续性管理体系	BSI（英国标准协会）	ISO 22301 是国际公认衡量企业服务连续性能力是否满足社会责任和客户承诺的权威标准。 该标准旨在预防、减轻、响应破坏性事件并从中快速恢复关键业务功能，降低业务中断风险和损失。

	ISO 38505-1 数据治理管理体系	BSI（英国标准协会）	ISO 38505-1 全球首个专门针对数据治理的管理标准，旨在指导组织有效，高效和可接受地使用数据，实现数据价值的最大化，同时保障数据及其应用过程中的运营合规与风险可控。
国内权威	可信云企业级 SaaS 服务能力	中国信息通信研究院	可信云企业级 SaaS 服务能力评估是由中国信息通信研究院发起的一项权威认证体系，旨在评估企业级 SaaS 服务在数据安全、服务质量、运营能力、权益保障、可定制、可集成等指标是否满足可信云服务评估规范和要求。
	网络安全等级保护三级	杭州市公安局	上上签电子签约云平台为业内首个通过等级保护三级测评。 网络安全等级保护测评，是遵从网络安全等级保护制度，贯彻落实《中华人民共和国网络安全法》，履行安全保护义务的要求，旨在保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

3.2 隐私保护

在数据治理框架下，我们已采取符合业界标准、合理可行的安全防护措施保护个人信息，包括数据分类分级保护、数据生命周期管理、零信任网络访问和数据防泄露解决方案等。个人信息处理活动严格遵循告知同意核心原则，在建立业务关系的过程中，涉及处理个人信息的场景，数据采集和处理之前获得用户明示同意，且收集数据类型和数量限于实现处理目的所必需的最小范围。更多隐私保护政策，请查阅官网主页《隐私政策》。

通过个人信息保护影响评估（Privacy Impact Assessment，简称 PIA）识别贯穿数据生命周期活动的隐私风险，评估用于保护个人信息主体的各项保护措施的有效性，持续监控个人信息处理活动对个人信息主体合法权益造成不利影响的风险，并采取适当的措施消除或降低风险，确保将数据安全和隐私风险控制到管理层认为适当的水平。

4 基础设施安全

4.1 云平台安全

上上签电子签约云平台部署在国内知名的公有云上，根据云安全责任共担原则，云服务提供商确保其基础设施的不间断可用性和物理安全性。云服务提供商为上上签电子签约云平台提供的底层安全性符合金融级安全保护要求。

4.2 通讯安全

上上签电子签约云平台默认为客户提供安全的通讯环境，采用 HTTPS/TLS 进行数据传输，也推荐客户使用高版本安全协议进行通讯，保护数据的机密性和完整性。

4.3 网络安全

上上签生产网络、测试网络和办公网络物理隔离。生产网络环境采用 VPC 实现私有网络边界隔离。根据重要程度、业务特性等因素划分安全区域，通过网络防火墙（安全组）实现区域隔离和细粒度的访问控制。在网络边缘，使用网络防火墙、Anti-DDoS、Web 应用防火墙、网络检测和响应等安全组件来过滤网络攻击，并具有主动监控和警报功能。

4.4 主机安全

主机安全管理遵循服务最小化原则，仅开启业务所需的服务和端口。通过统一配置模板制作系统镜像并定期更新，确保其符合安全基线要求。

同时，部署主机自适应安全解决方案，通过资产测绘、漏洞管理、基线检查、入侵检测、病毒查杀、日志分析与安全警报等能力，实现风险预防、威胁检测、事件响应与溯源的安全运营闭环。

4.5 密钥管理中心

密钥管理中心（KMC）基于国家密码管理局认证的硬件安全模块（HSM）来生成和保护密钥，为平台提供密钥生命周期管理服务，是电子签约云平台实现“明文不落地”的关键基础设施。

KMC 将密钥托管在 HSM 中，利用硬件机制来保护明文的密钥材料不会离开 HSM 的安全边界。使用 HSM 密钥进行运算时，密码运算的过程只会发生在 HSM 中，从而保证密钥的私密性，满足高等级安全要求。

5 数据安全

5.1 数据收集

为保障用户可正常使用我们的产品/服务，上上签在用户明示同意的前提下遵循最小必要原则收集个人信息。更多信息请查阅官网主页《隐私政策》。

5.2 数据传输

用户设备与上上签电子签约云平台之间的往来数据默认采用 HTTPS/TLS 进行加密，保护数据的机密性和完整性。

5.3 数据存储

电子签约平台不存储产品使用过程中产生的临时文件。

电子签约平台通过字段级和文件流加密来保障数据安全性。证件号采用 SM4 加密存储；图片与合同文件采用 AES256 加密存储，一文一密。

5.4 数据使用

上上签不使用真实个人信息进行测试，除非用户主动要求并授权。电子签约平台应用日志可能包含个人信息，日志记录的敏感信息将被脱敏或匿名化处理。

5.5 数据销毁

上上签 App 和 Web 端用户中心均提供账号注销功能。在主动注销账户之后，根据适用法律的要求，用户相关数据将被不可撤销地删除。

6 运营安全

6.1 安全开发流程

为了在快速迭代的过程中持续保障产品的安全性，上上签参考业界 SDL 理念，结合自身的开发实践和经验，形成一套规范的软件生命周期管理流程，并不断优化完善。

安全开发流程：

- 人员培训环节：安全设计要求、安全开发要求、编码规范、安全测试、隐私保护等，提升开发效率、软件质量与安全性；
- 需求评审环节：确认产品需要交付的安全需求，安全与隐私合规评审，确保交互设计符合安全实践；

- 安全开发环节：代码审查、代码安全性检测、软件成分分析等手段来避免非预期或恶意行为，减少软件中潜在安全漏洞的数量；
- 测试验收环节：自动化功能与安全用例测试、渗透测试，确保安全风险和隐私保护符合安全性保证；
- 项目发布环节：平台化流程发布上线，自动化质量阀控制，存档所有发布相关记录；
- 运营监控与响应：数据监控管理平台和安全响应中心 SRC 持续跟踪、监测，及时响应并处置发现的安全问题。

6.2 漏洞管理

上上签采用多种途径或手段监视内外部安全漏洞，包括但不限于使用商用及定制化工具定期自动执行内外部网络安全扫描、独立外部审计、第三方渗透测试、安全响应中心 SRC、威胁情报订阅等方式主动发现安全威胁。一旦确定某项漏洞需要进行处置，安全团队会记录在案并根据风险严重程度分配优先等级，之后推送至相关软件开发工程师或团队 Leader 进行处理。安全团队负责追踪该问题并持续跟进，直到确认问题已修复。

安全团队还与供应商、安全公司、白帽社区保持合作与沟通，并不定期邀请资深专家就漏洞生命周期各环节等相关议题进行现场交流。

6.3 事件管理

建立事件响应流程，以应对各类可能影响系统或数据机密性、完整性和可用性的信息安全事件。一旦发生相关事件，事件响应团队会根据事件性质、严重程度与影响范围进行记录与优先级排序，直接影响客户的事件被视为最高优先级。事件响应流程规范了应对工作的通知、升级、缓解与文档记录要求。

定期对事件响应团队的关键成员进行相关技能培训，对各类场景应急处置预案进行测试与演练，以检验预案措施的有效性。为快速响应与处置各类突发事件，事件响应团队全天候待命，可随时支援请求。

上上签依照相关法律法规和监管机构的要求，处理信息安全事件的通知及信息披露水平。我们提供及时、清楚且准确的事件通知，以便客户可以评估事态，必要时采取适当的、有效的措施。在成功实施补救措施或缓解方案后，事件响应小组负责对安全事件的原因、类型、损失与责任进行鉴定，制定纠正措施或安全整改计划，形成信息安全事件调查报告，总结经验教训。

6.4 权限管控

建立严格的访问控制机制来限制对电子签约平台资源的访问，员工默认无任何平台资源的访问权限。

账号授权遵循最低权限与需要知道原则，权限级别由其职位与角色决定。运维人员通过流程申请获得日常工作所需的权限，可审计与追溯。平台访问通过云堡垒机实现统一接入、统一管理、统一审计，并强制使用 MFA 进行身份验证，关闭下载通道，平台数据无法下载到本地，贯彻执行“生产数据不出生产”原则。

6.5 供应链安全

通过制定《供应商服务类别》和《第三方管理程序》规范供应商的管理，减低或控制第三方信息安全风险及服务持续性风险。在引入第三方供应商之前及之后，对其所能提供的安全性与隐私性、业务连续性等进行持续评估，确保符合供应商交付协议的信息安全和服务交付水准。

若涉及个人信息处理活动，与第三方供应商的合同条款会明确数据的来源、使用目的与范围，以及保密责任和义务，包括退出机制、数据清除期限、审计权利等。

6.6 业务连续性与灾难恢复

上上签电子签约云平台采用同城双活，异地容灾架构。同城双活数据中心同时提供服务，所有服务均冗余部署消除单点故障，采用弹性伸缩技术自动扩容，并实现流量自动负载和服务故障转移，有效保障业务的可靠性。

双活数据中心满足全量切换，提供跨中心业务负载均衡运行能力，实现持续的应用可用性和灾难备份能力。

异地容灾数据中心采用专线连接实现数据实时复制，保障重大灾难等极端情况下的业务连续性。

通过年度业务连续性计划的测试与演练，验证业务连续性措施的有效性，发现不足之处，总结经验，持续改进。

7 结语

信息安全是上上签的生命线。我们始终以安全为基石，以可靠为准则，持续优化产品和服务，不断提升用户体验，为构建更加高效、智能、可信的数字生态贡献力量。