上上签电子签约云平台

安全白皮书

版本：V4.0

发布时间：2021 年 3 月

目录

【声明】

本文档仅作为读者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，本文档内容会不定期进行更新，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

长期以来，上上签致力于保护用户数据的安全性和隐私性，也充分认识到信息安全对公司发展的战略意义。为此，上上签参考业界先进的云安全理念和安全实践，结合自身在云安全领域的技术积累与运营实践，构建纵深防御与合规遵从的安全保障体系并持续优化。本白皮书旨在介绍上上签电子签约云平台在安全性、合规性与隐私性方面的策略、流程和控制措施。

2 安全组织和人员

2.1 安全组织

上上签把信息安全作为公司重要战略之一，通过建立自上而下的信息安全管理组织架构来实现。在组织架构方面，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。

上上签安全团队包括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。工作职能包括建立及维护信息安全管理体系、监控与维护安全基础设施、开发安全审查流程、产品设计评估、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 员工背景调查

在正式加入我们的团队之前，上上签会验证应聘人员的教育背景和工作经历。在法律法规允许的情况下，上上签也可对应聘人员进行刑事、信用及安全背景调查，具体程度取决于应聘人员的职位。

2.2.2 保密协议

新员工入职须签订劳动合同和保密协议，明确员工对于履行职责中知悉的商业秘密与个人信息有保密责任和义务，且不因合同终止而结束。

2.2.3 全员安全培训与宣导

持续安全培训作为上上签信息安全策略的重要组成部分，贯穿全体员工就职期间。安全培训与宣导的形式与内容，包括但不限于：

- 在入职期间，新员工参加“新员工安全意识培训”项目，培训内容包括信息安全基本知识、信息安全行为守则和奖惩机制等。
- 采用多种途径宣传安全意识和安全行为守则，如在办公区域布置信息安全海报、制作《安全小报》并通过邮件传达至员工等。

- 每年开展面向全体员工的信息安全活动周，宣传最新信息安全资讯及案例等，并通过上上签网络学院平台进行考核。
- 根据职位或具体职能方向，员工可能需要接受与安全领域特定方向相关的额外培训。例如：网络与信息安全技能、安全编码实践、安全工具等专业知识。

3 安全合规与隐私保护

3.1 安全合规与标准遵从

上上签致力于保护用户数据的安全性和隐私性，并通过安全合规与标准遵从融入产品设计与安全运营，持续优化整体安全能力和业务保护水平，维护与客户的可信任关系。

至目前为止，上上签通过的安全测评与认证如下表所示：

资质		测评/颁证机构	简介
国际标准	ISO/IEC 27001 信息安全管理体系认证	BSI（英国标准协会）	ISO/IEC 27001 是被广泛采用的全球安全管理体系标准，其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管理标准的要求。 通过此认证，表明上上签对信息安全的承诺，致力于保障自身及客户信息的机密性、完整性和可用性。
	ISO/IEC 27018 公有云个人信息保护管理体系认证	BSI（英国标准协会）	ISO/IEC 27018 是首个专注于云上个人数据保护的国际标准，基于 ISO/IEC 27002 信息安全保护实用规则，同时针对适用于公有云个人可识别信息 PII 保护的要求。 通过此认证，表明上上签在保护企业数据、知识产权、个人信息等方面达到了高标准的行业实践。
	ISO 38505-1 数据治理认证	BSI（英国标准协会）	ISO 38505-1 数据治理旨在指导组织有效，高效和可接受地使用数据，保障数

			据及其应用过程中的运营合规、风险可控和价值实现。 通过此项认证表明上上签在数据资产的安全管理、数据使用的安全管控、数据治理的安全稽核等方面已建立系统性的治理框架来保障数据安全。
	ISO 22031 业务连续性管理体系认证	BSI（英国标准协会）	ISO 22301 是国际公认的，衡量企业服务连续性能力上是否满足社会责任和客户承诺的权威标准。 通过此认证，表明上上签已建立一套系统性的运行管理体系，识别潜在威胁，并提供一个有效的管理机制来阻止或抵消这些威胁，减少灾难事件给客户和组织带来损失。
国内权威	可信云企业级 SaaS 服务	中国信息通信研究院、云计算开源产业联盟	可信云服务评估是中国信息通信研究院下属的云计算服务评估品牌，也是中国针对云计算服务的权威评估体系。 通过此项认证，表明上上签电子签约云平台企业级 SaaS 服务在数据存储持久性、数据可销毁性、数据私密性、数据知情权、用户安全性、服务可用性等指标满足国家权威机构的评估规范和要求。为用户选择安全、可信的服务商提供信用支撑。
	公安部信息安全等级保护 2.0	杭州市公安局	网络安全等级保护要求是开展信息安全工作的管理规范和技术标准，已成为各行业广泛遵循的通用安全标准。 通过此项评测意味着上上签重视国家信息安全保障工作的基本制度，遵循信息安全等级保护管理规范和技术标准开展网络系统的建设与运营，履行安全保护义务，保障用户数据安全。

	工信部云计算服务能力标准三级	中国电子工业标准化技术协会	云计算服务能力评估由工信部牵头，围绕云计算服务中人员、技术、流程、资源、性能等关键环节进行能力测试，为最终用户选择和评价云服务提供参考依据。 通过此项测评表明上上签电子签约云平台企业级 SaaS 服务各阶段生命周期（咨询设计、部署实施、服务运营、持续改进、监督管理）及核心要素的规范性与可信赖程符合国家标准的要求。

3.2 隐私保护

上上签重视和遵守国家信息安全保障工作的基本制度，采取符合业界标准的安全防护措施保护个人信息安全，并持续优化个人信息管理和保护水平。

上上签通过国内外权威机构的评测与认证充分证明个人信息保护的能力。个人数据处理的技术和组织措施，包括但不限于：

- 设立隐私保护团队，开展隐私相关工作，保障用户的隐私权利；
- 建立多层防御体系，使得整体安全不依赖于单一的防御机制；
- 实施有效访问控制与监控机制，发现可能的违反政策行为；
- 采用加密与脱敏技术提高个人信息的安全性；
- 持续的第三方供应商风险评估缓解供应链的安全风险；
- 周期性第三方安全公司进行渗透测试发现并修复漏洞；
- 周期性 PII 风险评估，强化个人信息的保护措施；
- 定期举办信息安全和隐私保护培训课程，提高员工对于保护个人信息重要性的认识。

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、具金融级资质的公有云上，根据责任共担原则，云供应商确保其云服务平台基础设施的安全性，包括物理机房、计算、存储、网络设备等，云服务商为上上签电子签约云平台提供了底层安全性。

4.2 网络安全

上上签实行生产网络、测试网络和办公网络物理隔离。生产网络采用VPC，根据重要性、功能等因素划分区域，通过安全组及安全规则实现更细粒度的网络隔离，并部署 Anti-DDoS、WAF、NDR 安全系统来检测与防御网络与应用层的攻击行为。

4.3 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，确保符合安全基线要求。

同时，部署主机安全解决方案，通过资产管理、漏洞管理、基线检查、入侵检测、病毒防御与日志分析等安全能力，实现风险预防、威胁检测、事件响应与溯源的安全运营闭环。

4.4 密钥管理中心

上上签密钥管理中心（KMC）为平台提供密钥全生命周期管理服务，是上上电子签约云平台实现“明文不落地“策略的关键基础设施。

5 数据安全

5.1 数据收集

当用户使用上上签服务时，为保障用户正常使用我们的服务，上上签会在用户明示同意的前提下收集必要的个人数据。数据收集遵守公开透明和最小必要原则。上上签在《隐私政策》中披露了详尽的数据收集与使用政策。

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

上上签不存储产品使用过程中产生的临时文件。

上上签通过字段级和文件流加密来保障数据的安全性。证件号采用国密算法 SM4 进行加密存储；图片与合同文件采用 AES256 加密存储，一文一密。

5.4 数据使用

上上签不会用真实的 PII 进行测试，除非用户主动要求并授权。平台运行日志可能包含 PII，按要求写入系统日志 PII 被脱敏处理。

5.5 数据销毁

在符合当地法律法规的前提下，用户的数据删除申请通过之后，上上签启动数据销毁程序，用户的数据将被不可撤销地删除，以最大限度保证用户数据安全性。

6 运营安全

6.1 安全开发流程

为了在产品快速迭代的过程中持续保障应用安全，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，并在实践中持续优化不断完善。

安全开发基本流程：

- 人员培训环节：为开发人员提供代码开发规范、安全技能等培训，提高开发人员的安全意识，提升编码规范性和可维护性；
- 需求分析环节：根据需求文档识别产品需要交付的安全需求，聚焦安全性和隐私性；
- 安全开发环节：以安全红线、编码规范、设计标准为指导，并使用自动化代码检测工具进行扫描；
- 安全测试环节：工具化黑白盒测试，并结合人工 Code Review 降低代码缺陷和漏洞带来的安全风险；
- 项目发布环节：流程化平台发布上线，统一上线检测流程，存档所有相关数据；
- 运营与响应：通过运营监控平台与安全响应中心 SRC 进行跟踪、分析与处置。

6.2 漏洞管理

上上签通过多种途径或手段监视内、外部安全漏洞，包括但不限于采用商用及定制化工具定期执行内外部网络安全扫描、第三方渗透测试、安全检查与外部审计、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严重程度分配优先等级，之后推送至相关团队 Leader 或个人进行处理。安全团队追踪该问题并持续跟进，直到确认问题已得到修复。

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相关话题进行现场交流。

6.3 事件管理

为了应对各类可能影响系统或数据保密性、完整性和可用性的安全事件，上上签制定了《信息安全事件管理程序》。一旦发生相关事件，应急响应团队会根据事件性质、严重程度进行记录与优先级排序。直接影响平台核心功能的事件被视为最高优先级，程序指定了应对工作的通知、逐级处理、缓解与文档记录要求。

上上签定期组织对事件响应预案进行演练与测试，并对涉及的员工进行相关技能培训，以确保响应预案得到有效执行。应急响应团队全天候随时待命，以快速回应与处置各类突发事件。

对于涉及用户数据的安全事件，上上签将根据标准流程通知相关客户。在影响排除或采取必要措施后，应急响应小组负责对事件的原因、类型、损失、责任进行鉴定，制定后续跟进措施或纠正措施，形成《信息安全事件调查处理报告》，总结经验教训，持续改进。

6.4 网络访问控制

上上签设置严格的访问控制机制限制对平台资源的访问，员工默认无任何平台资源的访问权限。

运维人员通过流程审批获得日常工作所需的权限，遵循最低权限与必要悉知原则，访问权限或级别由其职位与角色决定，并强制采用 MFA 进行身份验证。通过堡垒机实现统一接入、统一管理、统一审计，并关闭下载通道，平台数据无法下载到本地，贯彻“生产数据不出生产”的原则。

6.5 供应商管理

上上签通过制定《供应商服务类别》与《第三方供应商管理程序》规范对供应商的管理。在引入第三方供应商之前，上上签会对其所能提供的安全性与隐私性、业务连续性水平等进行评估，确保第三方供应商能够提供与其服务范围及产品功能相匹配的安全性与隐私性保护能力。

对于涉及个人信息，合同条款中会明确数据的使用范围，以及保密责任和义务，包括退出机制、数据清理期限、审计权利等保障承诺。

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，实现流量负载均衡和服务故障转移，并采用弹性伸缩技术提高可靠性。

双活数据中心和异地容灾数据中心采用专线连接实现数据实时备份，保障重大灾难等极端情况下的数据安全。

此外，上上签还制定了业务连续性计划，并定期进行演练与测试，以验证业务连续性策略和解决方案的有效性，并形成正式的演练总结报告，其中包括结果、建议和实施改进的措施等。

7 结语

信息安全是上上签的生命线，上上签将持续以优质的产品与服务，不断完善的安全保障体系保护用户的数据安全，树立电子签约行业的安全标杆，推动行业的不断进步。