草料二维码数据安全白皮书

发布单位：宁波邻家网络科技有限公司

发布日期：2025 年 04 月 25 日

版本修订记录		
日期	修订内容	版本
2019 年 5 月	版本创建	V1.0
2020 年 8 月	增加信息安全等级保护资质说明，进一步细分关于阿里云公有云服务的技术安全描述。	V1.1
2023 年 7 月	增加 DCMM 认证资质	V1.2
2024 年 8 月	增加关于渗透测试服务的说明	V1.3
2025 年 4 月	补充“第三章、平台安全功能”，帮助用户了解草料功能层面提供的数据安全能力	V1.4

目录

一、 概述

草料二维码，是由邻家网络科技运营的一款以二维码为核心的无代码开发平台，通过灵活的功能模块和开放的底层 API，为客户提供二维码生成美化、业务系统搭建、数据管理与权限控制等功能，帮助用户实现低成本、高效率的业务数字化。查看官网

二、 安全合规

1. 国家标准制定者

国家质量监督检验检疫总局、国家标准化管理委员会在《中华人民共和国国家标准公告》（2017 年第 18 号）中正式发布《商品二维码》（标准号 GB/T 33993-2017）国家标准。草料二维码作为唯一受邀起草单位，参与了该标准的编制，为提升商品二维码应用的一致性与规范性作出贡献。

2013 年，草料二维码作为名片二维码国家标准起草组成员，协助编码中心共同制定了《二维码名片通用技术规范》（标准号 GB/T 31022-2014），该标准规定了名片二维码的数据结构、符号、信息处理和符号质量要求，适用于名片二维码的生成、印刷、识读和信息交换，将对规范我国二维码名片格式、推广二维码应用起到重要作用。


ICS 35.040
A 24

中华人民共和国国家标准

GB/T 31022—2014

名片二维码通用技术规范

General technique specification for two-dimensional barcode business card

2014-09-03 发布　　2015-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

ICS 35.040
A 24

中华人民共和国国家标准

GB/T 33993—2017

商品二维码

Two dimensional code for commodity

2017-07-12 发布　　2018-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

图 2.1 二维码国家标准

2. 等保三级认证

草料二维码严格遵守《GB/T 22239-2019 信息安全技术 网络安全等级保护》基本要求（简称“等级保护”），该标准由中国国家标准化管理委员会发布，是国家信息安全保障的基础性制度。等级保护制度根据信息系统的重要性与业务需求，将安全保护分为 1 至 5 个级别，由低到高实施不同的保护策略与管理要求。草料二维码系统已通过公安部门组织的信息安全等级保护三级（等保三级）测评，获得国家权威机构的认可与备案。这表明草料二维码已建立起符合国家标准的完备安全防护体系，能够有效保障用户信息安全与业务连续性，满足政企客户对于信息安全的合规性要求。

图 2.2 等保三级证书

3. DCMM 二级认证

数据安全管理能力成熟度评测（DCMM）是中国首个数据管理领域国家标准，根据《GB/T 36073-2018 数据管理能力成熟度评估模型》 的标准，草料二维码已获得 DCMM 二级 认证。该认证表明草料二维码已建立标准化的数据管理流程，包括 数据治理、数据安全、数据质量、数据架构 等关键能力，保数据资产在采集、存储、处理与使用全

过程中具备高度的安全性与可靠性。

图 2.3 DCMM 二级认证证书

4. 人员安全

草料二维码在数据安全管理方面，建立了完善的组织架构和制度体系，以确保平台和用户数据的安全性与合规性。

4.1 组织架构与职责分工

草料二维码设立了由 CEO 牵头的数据安全管理小组，统筹信息安全战略的制定与实施。质量保证部门作为信息安全管理的执行机构，负责日常的安全运营与技术防护。法务和综合部门则在合规审查、员工管理等方面提供支持，确保安全策略的全面落实。

4.2 员工全生命周期安全管理

在人员管理方面，草料二维码实施全生命周期的权限管理机制。 所有员工入职时均签署保密协议。同时对关键岗位员工进行背景调查，并且要求提供无犯罪记录证明，确保员工了解并遵守信息安全政策。 在职期间，公司定期开展信息安全培训和教育，提升员工的安全意识和操作规范。 员工离职时，及时注销账号、回收信息资产，防止数据泄露风险。

4.3 制度规范

草料二维码依据国家政策法规和行业最佳实践，构建了覆盖数据全生命周期的管理制度。 该制度涵盖安全评估、数据分级分类、数据脱敏、流程审批等关键环节，确保信息安全工作的系统性和可持续性。

4.4 第三方安全服务

草料二维码与阿里云服务团队、广电计量等第三方检测机构合作，定期进行安全检测、渗透测试、数据安全评估，识别并修复潜在的安全漏洞，提升平台的整体安全防护能力。

三、 平台安全功能

1. 账号与身份安全

1.1 账号实名认证

平台支持账号实名认证，用户完成认证后，若需找回账号或进行审核等操作，需提交与认证主体一致的资料进行验证，增强账号的安全性和可追溯性。

1.2 账号变更验证

为防止账号被恶意篡改，草料二维码在用户更换登录手机号时，要求通过原手机号进行验证，确保账号控制权的合法转移。

1.3 多设备登录提醒

为加强账号安全管理，草料二维码引入了多设备登录提醒机制。当系统检测到同一账号在多个浏览器或设备上同时登录时，平台会主动弹出提示，提醒用户当前账号已在其他设备上处于活跃状态。 此提醒是为了帮助用户识别潜在的账号共享或异常使用行为，提醒用户采取更换密码、设置成员权限等措施。强化账号的安全防护，确保用户数据的安全性和操作的合规性。

2. 二维码内容访问控制

2.1 成员访问权限设置

草料二维码允许用户为每个二维码设置特定的查看权限，仅授权的成员可以访问二维码内容，防止信息被非授权人员查看。

2.2 访问密码保护

用户可为二维码设置访问密码，只有输入正确密码的人员才能查看二维码内容，增加了信息的保密性。

2.3 访问时间段限制

平台支持设置二维码的访问时间段，用户可指定每天的特定时间段允许访问，超出时间段则无法访问二维码内容，适用于限定时间的信息展示。

2.4 访问地区限制

草料二维码提供基于地理位置的访问控制功能，用户可设置二维码的可访问地区，非指定地区的访问请求将被拒绝，增强了信息的地域性安全控制。

3. 操作权限与审计管理

3.1 操作权限分配

超级管理员可根据业务需求，为不同角色的成员分配相应的操作权限，包括工作台管理、表单填写、状态面板操作、动态数据查看等，确保成员仅能访问和操作其职责范围内的内容。

3.2 成员权限管理

为确保组织成员的账号安全和权限管理，草料二维码平台支持为每位成员分配独立的账号和权限，避免多人共享账号带来的安全风险，确保操作的可追溯性和责任明确。在成员离职等情况下，管理员可直接在成员列表中删除该成员，系统将自动取消其相应权限，防止前员工继续访问二维码或工作台。

3.3 分区管理与数据隔离

草料二维码提供分区功能。开启功能后，可以将账号划分为不同的分区，各分区之间的数据相互隔离，并可为成员分配不同的分区权限。尤其适用于多部门协作的场景，确保数据的安全性和独立性。

3.4 操作日志记录与审计

平台会记录每位成员的操作日志，包括操作时间、操作内容等信息，便于事后审计和问题追踪，提升系统的透明度和安全性。

4. 数据保护

4.1 二维码误删恢复功能

为防止重要数据的意外删除，草料二维码提供二维码误删恢复功能，用户可自助恢复被删除的二维码，保障数据的完整性。

4.2 数据删除二次确认

在用户删除二维码、表单数据、批量模板等重要内容时，草料二维码平台将弹出确认提示，明确告知删除操作的后果，并要求用户主动勾选“我已确认要删除数据”选项后方可继续执行。通过增加用户的确认动作，有效降低误操作风险，保障数据安全与操作的可控性。

4.3 区块链存证

草料二维码与蚂蚁集团合作，为用户提供区块链存证服务。该服务利用区块链技术的不可篡改性和时间戳特性，确保数据的真实性和完整性。功能开启后，每条表单记录或子码内容在提交后，系统会自动将其上链存证，生成唯一的存证哈希和时间戳。 存证数据可作为电子证据，具有法律效力，支持在司法场景中的证据采信。

即便用户在草料平台中删除了原始数据，存证哈希及区块链上保存的信息依然完整保留。用户可通过存证核验服务验证提交数据的真实性，查询原始内容、提交人、提交时间等信息，确保数据具有持续的可验证性和不可否认性，进一步提升数据管理的可靠性与合规性。

5. 隐私保护与合规

5.1 表单字段隐私保护

草料二维码支持对表单中的敏感字段（如姓名、手机号、身份证号码等）进行匿名化处理，用户可选择开启隐私保护功能，自动隐藏部分内容，防止个人敏感信息的泄露。

5.2 敏感信息处理与合规措施

草料二维码在处理用户数据过程中，严格遵守《中华人民共和国个人信息保护法》等相关法律法规，始终坚持最小必要、合法正当、公开透明的原则，采取多项技术与管理措施保护用户的敏感信息安全。我们通过加强数据加密传输、访问权限控制、异常监测与审计留痕等手段，确保数据在采集、存储、使用、传输和删除各环节的安全性与合规性。详细的数据收集与使用规则，请参考《隐私政策》。

四、 底层技术安全

草料二维码基于阿里云基础架构服务，采用金融级安全标准，从数据传输、存储隔离、访问控制、灾备与高可用、风险防护等多个层面，建立了完备的技术安全保障体系，持续保护用户数据的机密性、完整性与可用性。

1. 云基础架构与网络安全

专有网络隔离（VPC）：通过阿里云 VPC 实现生产环境与测试环境的物理隔离，严格限制非授权 IP 访问，降低攻击面。

网络边界防护：部署安全组策略和 DDoS 防护机制，有效抵御网络层攻击，保障服务稳定性

数据库安全访问：数据库实例仅开放内网白名单访问，关闭公网入口，防止外部入侵。

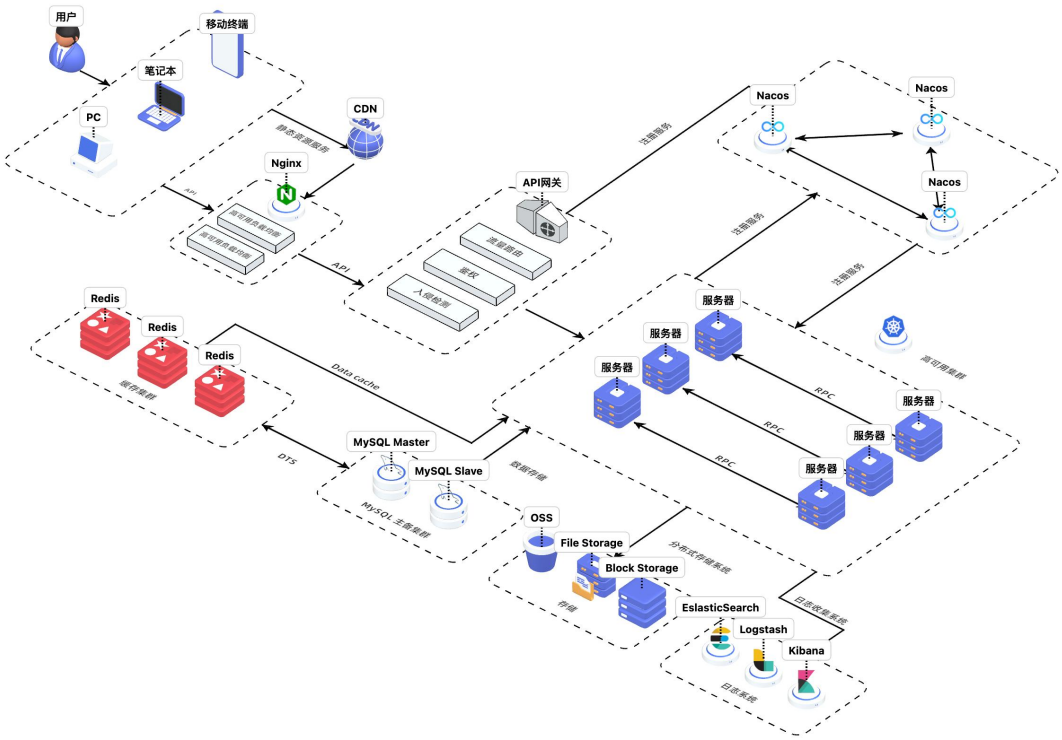

图 4.1 草料二维码系统架构

2. 应用与数据传输安全

应用层防护：部署 Web 应用防火墙（WAF），防御 SQL 注入、跨站脚本（XSS）等常见应用层攻击，保护 Web 应用安全。

加密通信：所有用户端与服务器通信采用 HTTPS/TLS 1.3 协议，强制 SSL 加密，防止中间人攻击。

API 安全机制：关键接口通过阿里云 API 网关签名机制校验请求来源，防止接口滥用和伪造请求。

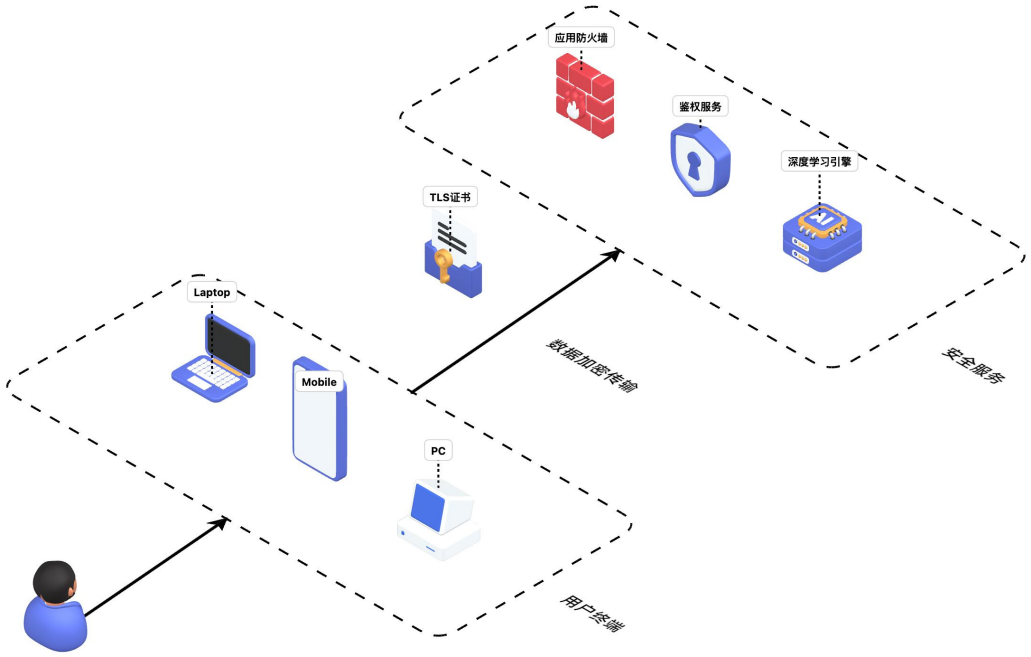

图 4.2 草料二维码应用安全服务

3. 数据存储与访问控制

全链路加密：数据在传输与存储过程均加密处理，保障数据在流动和静止状态下的安全。

多层权限控制：基于阿里云 RAM 资源访问管理，按照最小权限原则为开发、运维、第三方服务分配角色权限。

多因素认证（MFA）：关键操作如数据导出、配置变更需启用 MFA 保护，提升账户安全

性。

4. 数据隔离与脱敏保护

租户级资源隔离：通过阿里云租户级资源隔离，确保不同客户数据物理或逻辑隔离，杜绝跨用户访问。

敏感数据脱敏处理：采用不可逆哈希算法对敏感数据进行脱敏存储，降低数据泄露风险。

5. 容灾备份与高可用设计

多可用区部署：核心业务部署于多可用区，数据库采用主备高可用架构，提升系统冗余性与稳定性。

弹性伸缩与负载均衡：通过 SLB 负载均衡与 Auto Scaling 自动扩缩容机制，应对突发流量压力，保障业务连续性。

灾备演练与实时监控：定期开展全链路灾备演练，配合阿里云云监控与日志服务（SLS）实时监测异常，快速定位与处置故障。

6. 风险防护与威胁检测

云安全中心：部署威胁检测、漏洞管理、入侵防御、日志审计等全栈式安全防护体系，构建主动防御能力。

漏洞扫描与修复：定期扫描服务器与中间件组件（如 Nginx、Redis）漏洞，生成修复建议并跟进处理。

入侵检测与基线检查：通过行为分析识别异常行为，自动隔离恶意进程；持续校验服务器配置，符合 CIS 国际安全标准。

7. 定期渗透测试

草料二维码定期委托阿里云安全团队进行渗透测试（Penetration Test），阿里云安全团队会以攻击者思维，模拟黑客对业务系统进行全面深入的安全测试，帮助企业挖掘出正常业务流程中的隐藏的安全缺陷和漏洞，并提出修复建议。提升安全防护体系的防御能力。[了解阿里云渗透测试服务]

五、 草料二维码安全承诺

草料二维码始终将数据安全作为平台发展的基石，严格遵循国家法律法规和行业标准，构建了覆盖组织管理、平台功能、底层技术、合规保障的全方位安全防护体系。

通过持续的技术投入与管理优化，草料二维码致力于为每一位用户提供安全、稳定、可信赖的服务环境。在未来，草料二维码将持续关注网络安全领域的新技术、新威胁和新标准，不断完善安全治理体系，及时更新和加强数据保护措施，确保用户的数据资产始终处于安全、合规、可控的状态。

如果您对草料二维码的数据安全措施有任何建议或反馈，欢迎随时前往 草料二维码官网 联系我们。我们将以专业、积极的态度，持续推动平台安全能力的提升。