企迈安全白皮书

版本（V1.2）

2021 年 12 月 09 日

目录

版本记录

版本号	生效日期	修订说明
V1.0	2021–08–13	版本创建
V1.1	2021–10–16	新增并修改部分内容
V1.2	2021–12–09	新增并修改部分内容

一. 前言

企迈科技是企业级的 SaaS 服务提供商，从组建伊始就以为商家提供安全可靠的数字化服务为第一要务。因此团队不仅在安全工作上投入了大量的资源，而且也组建了专职专业的安全专家团队，致力于提升平台的安全表现，完成了诸如安全加固、升级、改造工作，保障并推广团队安全政策及措施的普及与落地等。

企迈 SaaS 功能包括机构成员管理、会员、商品、订单、小程序、卡券、聚合配送等功能等，产品具有高度的可扩展性与可用性。我们采用业界领先的技术，对产品、用户数据进全生命周期的安全保障。企迈产品的设计、开发和运营充分考虑了合规性以及用户个人信息隐私性要求，保证产品满足业务运营用户对安全合规性、个人隐私性以及数据保护的法律法规和原则要求。

二. 安全保障

1. 安全专员团队

企迈科技组建了平台安全保障组织架构，设立稳定性委员会及安全专家团队，通过系统安全、网络传输安全、数据存储安全、业务安全等领域精细分工，各司其职。安全团队还会关注整个平台需求、设计、研发、运维等整个生命周期的安全问题，及时发现隐患，防患未然。同时安全团队还致力于通过建立安全平台、代码走查、安全培训等措施，在整个团队中布道安全知识及规范，提升平台整体安全能力。

2. 安全日常职责

企迈科技的安全团队日常完成如下（不仅限于）职责：

1）及时响应外部安全平台提交的漏洞、入侵检测等，承诺 6 小时内解决上线。

2）关注产研团队在需求分析、系统设计、产品研发、运行运维过程中存在的安全隐患、给出改进方案、并指导与监督隐患的排除。

3）主动在测试、集成、生产环境中引入漏洞检测与扫描工具，及时发现安全漏洞并予以解决。

4）依据数据类别及安全等级，设计访问控制策略，通过技术手段制定隔离措施和访问控制管理流程。

5）依据业务系统访问逻辑，审核访问请求，自动化监控可疑活动（例如：数据的非授权访问及操作）并实时审计，定期复查其执行情况。

6）遵循信息安全事件管理标准，依据数据安全性的危害程度定义安全事件类别和响应流程，提供全天候人工和系统的监控识别、分析和处理信息安全事件的能力。

7）进行定期的安全演练，验证安全策略的有效性、可靠性和适用性。

8）定期为团队成员提供安全意识培训，包括个人准则、信息保护、数据安全认证和安全开发等内容。

3. 信息资产安全级别与管理机制

团队根据国家法律法规政策要求、按照业务价值、数据关键性、影响范围等维度对信息安全资产进行了细致评估。总体共计 7 大领域，每个领域设定了责任人、使用人、CIA 级别（保密性、完整性、可用性）及重要等级，做到专人专项管理及负责。

此外，团队还对信息安全事件进行了分级和定义，根据安全事件的影响程度和范围，制定了不同的管理机制、应对策略、处理及报告流程、总结汇报等。

三. 合规与隐私

1. ISO/IEC 27001:2013 信息安全管理体系认证

ISO27001 是一套获得业界广泛认可的安全管理体系标准，其一直被认为是国际最权威、最严格的信息安全体系认证标准，被全球广泛接受。企迈科技的数据中心、研发体系、职能部门通过此项认证意味着我们在信息安全管理领域已经与国际标准对标，具有充分的信息安全风险识别和控制能力，可以为全球客户提供安全可靠的服务。


信息安全管理体系认证证书

注册号：0350121IS20459ROM

兹 证 明

企迈科技有限公司

注册地址：合肥市高新区望江西路800号创新产业园C1楼10层，230088

统一社会信用代码：91340100MA2T68T689

管 理 体 系 符 合

GB/T 22080-2016 / ISO/IEC 27001：2013 标准

该管理体系适用于

与计算机应用软件开发相关的信息安全管理活动；《适用性声明》（版本号：V1.0）（边界：合肥市高新区望江西路800号创新产业园C1楼10层1005）***

颁证日期：2021年7月16日

有效期最长可至：2024年7月15日

签 发 人：

兴原认证中心有限公司

证书专用章

中国认可 国际互认 管理体系 MANAGEMENT SYSTEM CNAS C035-M

2. ISO/IEC 27017:2015 提供云计算信息安全方面的指导认证

ISO27017 是属于保护云服务安全的国际标准，属于云服务提供商的国际标准。是专门针对云计算服务的信息安全控制措施实用标准，为云服务行业提供了 ISO/IEC 27002 的指南，与 ISO/IEC 27001 标准配合使用，将有效加强对云服务提供商及云服务客户的管理能力。

企迈科技获得此项认证，是对我们长期以来在云安全体系建设方面工作的充分肯定。

3. 公安部信息安全等级保护三级认证

《GB/T 22239—2019 信息安全技术网络安全等级保护基本要求》简称网络安全等级保护，是中国国家标准化管理委员会发布的信息安全标准，是中华人民共和国信息安全保障的一项基本制度。等级根据信息系统的重要程度，从低到高分为 1至5 个等级，不同安全等级实施不同的保护策略和要求。企迈科技采用的是 3 级信息系统的保护策略，并通过了专业测评机构的测评认证。说明企迈科技提供的产品服务有能力帮助客户具备三级等保所要求的：安全事件 的发现、应对能力，信息系统受到破坏时的恢复能力。

信息系统安全等级保护备案证明

依据《信息安全等级保护管理办法》的有关规定，企迈科技有限公司 单位的：

第三级 企迈 SAAS 系统予以备案。

证书编号：34010100310-00001

中华人民共和国公安部监制

备案公安机关公章

二〇二一年十月 日

四. 生产过程安全

1. 保密要求

团队将严格遵守《中华人民共和国网络安全法》《中华人民共和国电子商务法》《个人信息安全规范》、《中华人民共和国计算机信息系统安全保护条例》《信息安全等级保护管理办法》等法律法规和规范性指导文件及服务协议，确保用户和商家的敏感信息及业务数据不被泄露。

此外，依据员工的工作角色进行额外信息安全培训与考核，法律政策宣导与普及、保密协议签署。并按照按岗位保密规范需要、最小力度授予安全权限、确保员工管理的用户数据按照安全策略执行。

2. 平台研发过程及运维安全

在 SASS 平台的设计、研发、运维、发布等环节中，不会使用生产环境的数据，从而造成用户信息及数据的泄露。

五. 系统安全

1. 系统配置安全

生产环境运行于阿里云统一版本的操作系统上，服务的安装、升级、迁移均由权限受限的运维人员完成，并从阿里云指定的可信任安装源下载。系统级服务如应用服务、nginx 网关、mysql 数据库、redis 缓存、MQ 消息队列等的配置文件则由配置中心统一管理，通过发布运维平台进行统一维护和下发。

2. 系统访问权限

对于生产环境的运维操作有专门运维平台，运维平台会维护运维人员的操作权限，并提供操作日志进行审计。

运维人员只能在必要情况下通过堡垒机登录服务器进行操作，并需要在运维平台中申请临时运维账号及权限，在通过审批后方可操作，相应权限会在运维完成后被及时回收。相关的权限审批、操作日志等均会被审计。

对于数据库与服务器账号密码等信息，则严格要求设置有效期、定期强制变更，确保账号密码的时效性与安全性。

3. 安全开发&运维流程

基于 ISO27001 框架标准、建立安全开发及运维框架与流程、并确定所有规范和流程定期执行。定期对全体人员进行安全方面的培训，巩固及完善安全意识。开发、测试、验收和生产环境严格隔离、每套环境采取独立授权机制。

六. 网络传输安全

1. 传输协议

为了防止中间人攻击，全站服务采用 https/SSL 加密数据传输，采用 RSA 算法进行密钥加密，签名算法则采用安全散列算法较高位数的 SHA-256，来保障密钥的不可破解性。

2. 安全域划分

企迈云平台所有产品部署都采用了 VPC（Virtual Private Cloud，虚拟私有网络），将应用服务、数据存储服务、Redis 与 MQ 等基础设施进行网络隔离。开发、测试、生产环境网络各自完全隔离、将各应用服务与数据传输、存储服务限制在各自的安全域中，保障业务服务与业务数据安全性。

3. 网络访问控制

在生产环境中，各子网间通过防火墙、安全策略组等机制，保证网络访问控制被限制在一定权限内。包括外部的上行出口，也进行统一化管理。

4. 安全防御

企迈科技采用了阿里云提供的 WAF 防火墙服务，能够有效地防止各类 DDOS 攻击、能够及时发现处理安全威胁。对于 WAF 的预警、运维人员会第一时间予以关注与处理。

5. 流量监控

对于图片、文件、静态资源等、企迈科技采购了阿里云的 OSS 服务、并设置了独立域名服务。并对请求的上下行流量进行监控，在确保不影响用户体验的前提下，能够及时发现异常请求，做降级限流处理。

七. 数据安全

1. 数据隔离存储

在企迈平台上，所有业务数据采取了水平分割的分库分表机制，确保了数据的互相隔离，防止被拖库的危险。同时数据库对访问账号进行了独立权限控制，避免越权漏洞导致数据被破坏。

2. 数据脱敏

所有业务敏感信息与用户敏感信息均采用对称算法加密进行了脱敏处理、在数据库中以密文形式存储，并定期更换对加密因子进行更换。

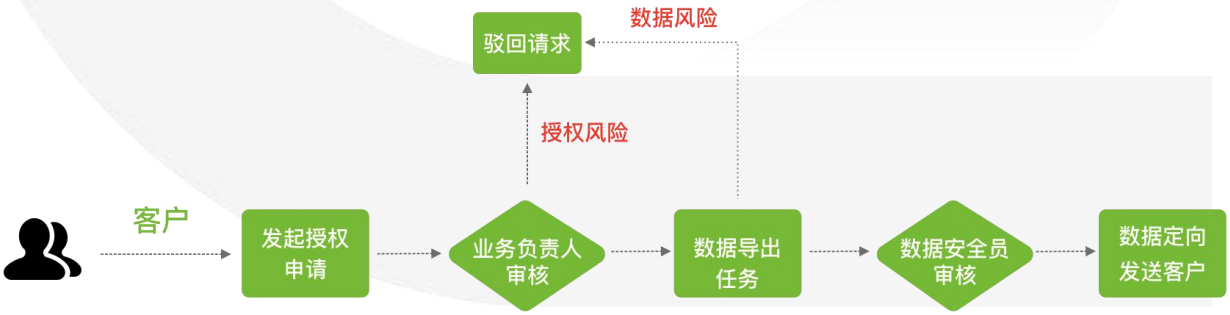
3. 文件存储

采用了阿里云提供的 OSS（对象存储服务）存储所有图片、附件、文档、公共资源等文件，具有扩容方便、安全及可靠性高等优点。

4. 生产环境数据权限

除非得到客户/用户授权，否则产研团队任何成员（包括运维人员）被禁止接触生产环境数据、 接触的形式包括但不仅限于数据库访问、导出、截图、拍照等途径。更不会私自窜改数据避免给用户造成信息泄露。安全专员定期对数据库操作日志进行审计。

在实际业务生产过程中、因为商家在业务统计上的特殊需要、需要企迈技术人员配合进行数据导出、经过商家授权、层层审批后、可定向数据提取。数据提取流出如下：



5. 数据销毁管理

对于长期无访问记录企业对应的数据，企迈科技承诺会在三年内予以保存，但逾期的数据存在被清理的风险。

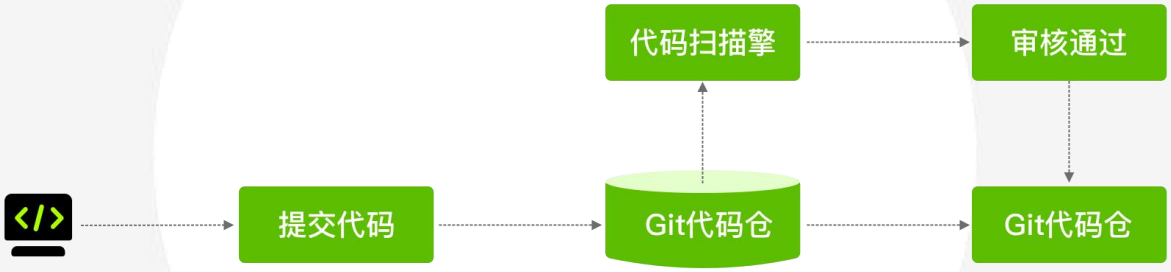
6. 数据备份安全

所有在线业务数据会进行实时备份、每天晚上也会对数据进行全量备份。并确保数据备份、业务数据统计等环节的数据安全。

八. 系统应用安全

1. 代码安全扫描

在测试、集成、灰度以及生产环境，所有产品代码部署之前、均经过了动态代码扫描工具，对整个平台的代码进行全面的扫描，防止出现 SQL 注入、XSS/CSRF 攻击等代码安全隐患、对不符合安全规范的代码禁止提交发布。



2. 接入安全

平台引入了阿里云的 WAF 防火墙，可在网络接入层阻断恶意请求，有效防止注入类及 XSS/CSRF 攻击请求。

3. 业务逻辑安全

在灰度以及生产环境所有产品需求发布均经过测试人员验收测试。并同时触发自动化测试、对业务链路进行全场景回归、确保所有发布的产品功能业务逻辑安全有效。

4. 接口访问安全

所有通过开发平台接口访问企迈产品的服务、均需要采用密匙验证机制、过滤不完全的非法请求。每个商家的每个应用接入方都有独立的密匙秘钥机制，确保每个三方调用的安全性。

九. 业务操作安全

1. 账号及密码安全

账号体系支持手机验证码与账号密码等方式登录。所有用户登录静态密码要求为 8 位以上，包含大小写英文及数字。平台会记录用户每次登录行为，生成常用 IP，若在非常用登录地点上登录，则会激活二次验证。账号系统会监控账号的异常操作，如多次恶意尝试登录、多次越权操作等，均会有实时告警并触发账号锁定操作。

2. 业务权限

业务系统提供了菜单级别、页面、按钮等多级别的权限管控机制。每个商家可以按照业务需求进行独立角色权限定义、并独立授权。每个商家的授权信息进行了隔离存储。

3. 日志审计

管理后台对用户访问、操作做详细的日志记录，所有记录保持一年有效，超过一年的将作归档处理。可以按照商家授权、将部分日志提供给企业管理员、运维人员进行审计，但需严格按照相关的审批流程。

4. 监控及告警

对于商家后台定向手动调整储值、定向手动发券、定向用户营销等功能作出实时监控预警、企迈安全人员进行排查。对超出业务预期的部分会向商家进行预警。