销售易安全白皮书

Neocrm 销售易

北京仁科互动网络技术有限公司

版权说明

文档变更记录

版本号	日期	变更人员	变更内容
1.0	2016年8月1日	销售易技术部	白皮书文档1.0版本
1.1	2016年12月28日	销售易技术部	内容更新
1.2	2017年3月5日	销售易技术部	内容更新
2.0	2017年10月10日	销售易技术部	白皮书文档2.0版本
2.1	2018年5月8日	销售易技术部	内容更新
2.2	2019年10月1日	销售易技术部	内容更新
3.0	2019年12月5日	销售易技术部	白皮书文档3.0版本
3.1	2020年3月20日	销售易技术部	内容更新
3.2	2022年3月3日	销售易技术部	内容更新

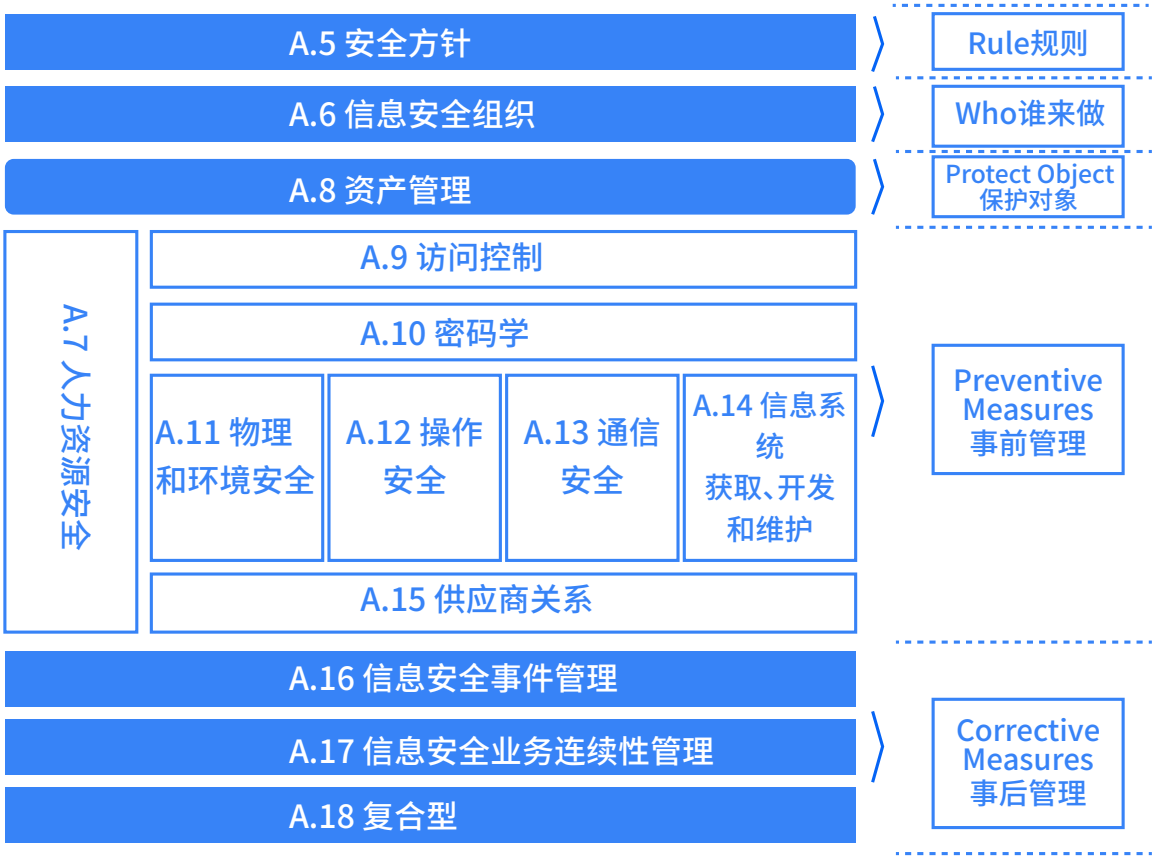
目录

一 销售易安全架构

1.1 27001信息安全管理体系（ISMS）

销售易在设计、建设安全管理体系过程中，参考了信息安全管理体系（Information Security Management System，简称为ISMS），它是从英国BS7799发展起来的信息安全领域中的一个最佳实践模型，是管理体系（Management System，MS）思想和方法在信息安全领域的应用。

近年来，伴随着ISMS国际标准的发展，ISMS迅速被全球接受和认可，成为世界各国、各规模组织解决信息安全问题的一个有效方法。ISMS认证随之成为企业和组织向社会及其相关方证明其信息安全水平和能力的最佳途径之一。



信息安全管理体系控制域分布

在ISMS的要求标准ISO/IEC27001:2013（信息安全管理体系要求）的第3章术语和定义中，对ISMS的定义如下：

ISMS（信息安全管理体系）：是整个管理体系的一部分。它是基于业务风险方法，来建立、实施、运行、监视、评审、保持和改进信息安全的。（注：管理体系包括组织结构、方针策略、规划活动、职责、实践、程序、过程和资源。）

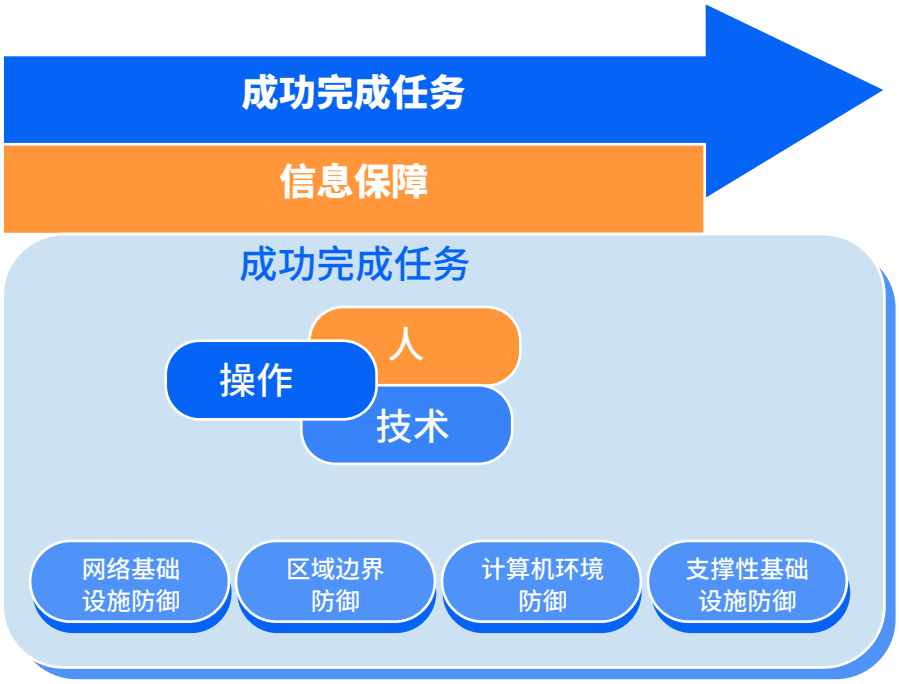
这个定义看上去同其他管理体系的定义描述不尽相同，但也可以用ISO GUIDE 72:2001（Guidelines for the justification and development of management system standards管理体系标准合理性和制定导则）中管理体系的定义，将ISMS描述为：组织在信息安全方面建立方针和目标，并实现这些目标的一组相互关联、相互作用的要素。

ISMS同其他MS（如QMS、EMS、OHSMS）一样，有许多共同的要素，其原理、方法、过程和体系的结构也基本一致。

单纯从定义理解，可能无法立即掌握ISMS的实质，可以把ISMS理解为一台“机器”，这台机器的功能就是制造“信息安全”，它由许多“部件”（要素）构成，这些“部件”包括ISMS管理机构、ISMS文件以及资源等，ISMS通过这些“部件”之间的相互作用来实现其“保障信息安全”的功能。

1.2 安全保障技术框架（IATF）

销售易在建设信息安全体系时，参考美国国家安全局（NSA）提出的信息安全保障技术框架（Information Assurance Technical Framework，IATF），如下图所示。



ITAF技术保障框架

IATF依据“深度防护战略(Defense-in-Depth)”理论，要求从整体、过程的角度看待信息安全问题，强调人(People)、技术(Technology)、操作(Operations)这三个核心原则，关注四个层次的安全保障：保护网络和基础设施(Defend the networks and infrastructure)、保护边界(Defend the enclave boundaries)、保护计算环境(Defend the computing environment)、支撑基础设施(Supporting infrastructures)。

IATF模型从深度防护战略出发，强调人、技术和操作三个要素：

人(People)：人是信息的主体，是信息系统的拥有者、管理者和使用者，是信息保障体系的核心，是第一位要素，同时也是最脆弱的。正是基于这样的认识，安全组织和安全管理在安全保障体系中是第一位的，要建设信息安全保障体系，首先必须建立安全组织和安全管理，包括组织管理、技术管理和操作管理等多个方面。

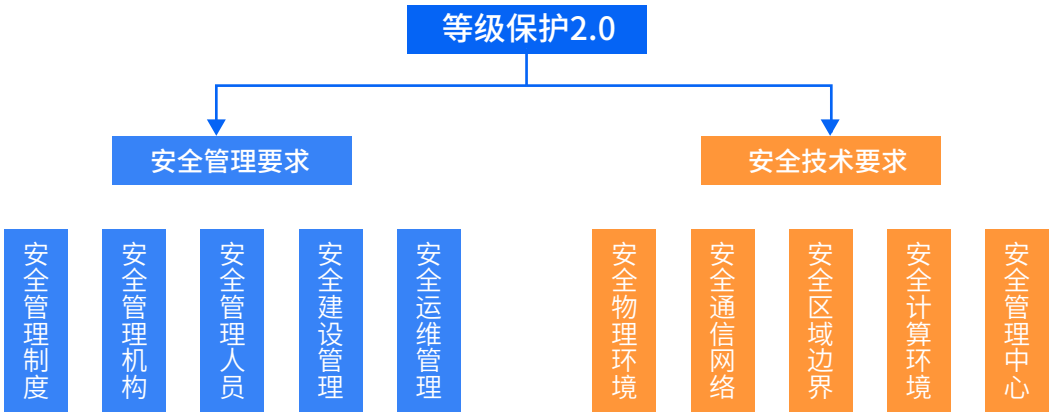
技术(Technology)：技术是实现信息安全保障的重要手段，信息安全保障体系所应具备的各项安全服务就是通过技术机制来实现的。当然IATF所指的技术是防护、检测、响应、恢复并重的动态的技术体系。

操作（Operation）：也可称之“运行”，它体现了安全保障体系的主动防御，如果说技术的构成是被动的，那操作和流程就是将各方面技术紧密结合在一起的主动过程，运行保障至少包括安全评估、入侵检测、安全审计、安全监控、响应恢复等内容。

信息安全保障体系的实现就是通过建立安全组织、安全管理和防护技术体系，协调组织、技术、运作三者之间的关系，明确技术实施和安全操作中技术人员的安全职责，从网络和基础设施、区域边界、计算环境、支撑基础设施等多层次保护，从而达到对安全风险的及时发现和有效控制，提高安全问题发生时的反应速度和恢复能力，增强网络与信息的整体安全保障能力。

1.3 等级保护安全体系

销售易在建设信息安全保障体系时，同时参考目前国内最新的等级保护2.0标准的三级要求，从安全管理、安全技术两大维度综合考虑，涵盖安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理、安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心十个子类。



等级安全保护2.0通用安全体系

1.4 销售易安全保障体系设计

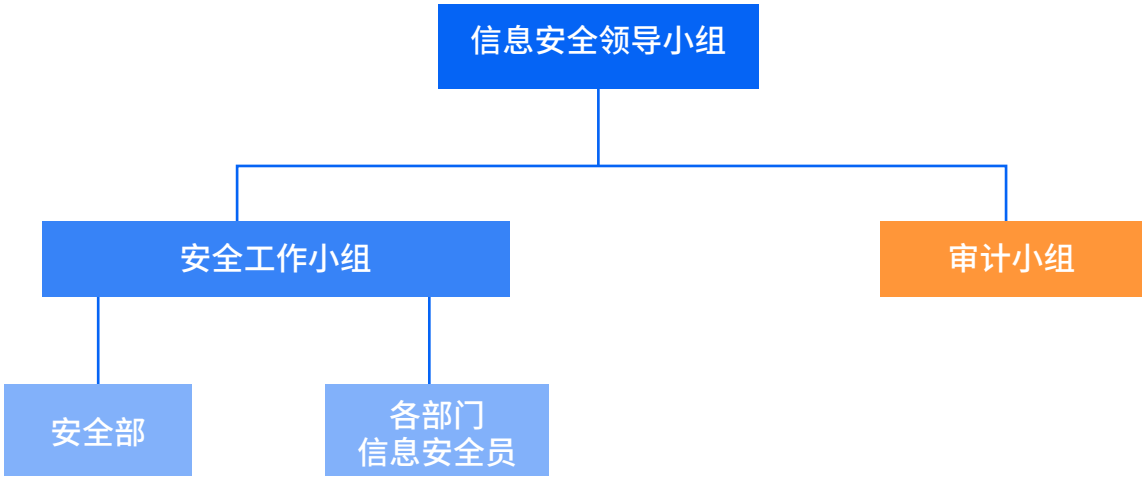
销售易信息安全保障体系的建设，以自身信息系统的实际情况和现实问题为基础，参照国际IATF、ISMS标准规范及国家信息安全等级保护的要求，充分利用成熟的信息安全理论成果，设计出兼顾整体性、可操作性，并且融合策略与组织、安全防护、安全监控、安全运行、应急恢复和品牌价值为一体的信息安全保障体系，保障销售易信息系统的安全运行。

销售易信息安全保障体系框架

二 管理与组织体系

2.1 安全组织架构

为了使信息安全工作在公司全面推行及落地，销售易成立了自己的信息安全组织机构，包括信息安全领导小组、下设信息安全工作小组和审计小组，架构如下：



安全领导小组职责：

- 全面负责和领导公司信息安全工作
- 提出公司信息安全工作目标和要求
- 审批公司信息安全策略方针和战略规划
- 定期接受信息安全审计工作及管理工作汇报
- 对紧急、重大安全事故进行决策响应
- 监督协调公司信息安全活动并提供必要支持

安全工作小组职责：

- 公司信息安全的规划、设计和建设，参与信息系统安全性评审
- 制定、维护和审视公司信息安全策略、标准、制度、制定信息安全管理流程和安全操作指导手册，并负责在全公司范围内推行落实

- 定期向决策层汇报公司信息安全状况及信息安全管理工作
- 公司信息安全状况的例行检查、监控，组织例外的检查和审计，协助外部审计工作开展，发现管理和技术上存在的安全漏洞隐患并进行改进
- 定期组织收集、整理、分析公司的安全状况和业界安全动态，提出安全预警报告和落实防范措施
- 对公司员工进行信息安全宣传、培训，提高员工的安全意识
- 成立各级信息安全事件应急小组，组织、协调重大信息安全事故的调查和解决

内审部工作职责：

- 安全工作小组工作成果跟踪和审计
- 负责组织开展公司信息安全内部审计工作
- 定期向决策层汇报公司信息安全审计工作
- 协助安全部推进落实公司信息安全管理规定

2.2 制度与流程

根据ISMS和ISO20000的要求，公司制定了一套完善的IT服务和安全管理体系规范，包括ISMS的14个领域（安全策略、安全组织、人员安全、资产安全、物理和环境安全、访问控制、密码管理、信息系统开发和获取、供应商管理、安全事件管理、业务连续性管理、符合性管理），同时涵盖了ISO20000体系的管理要求。（包括服务级别管理、服务连续性和可用性管理、供应商管理、事件和服务请求管理、问题管理、配置管理、变更管理和发布管理）。

2.3 信息安全团队建设

根据公司安全战略目标，销售易组建了一支专业的信息安全团队，具备了安全风险防范、发现、处置与应急响应的能力，其成员职责如下：

安全架构师

- 负责公司总体安全风险识别与管理
- 安全框架设计与执行落地
- 指导安全团队开展各项安全工作
- 各部门工作协调与安全工作汇报总结

渗透测试工程师

- 负责对业务系统开展渗透测试工作
- 负责代码漏洞扫描
- 负责代码人工审核

安全运维工程师

- 负责日志审计与监控
- 负责安全评估和加固
- 负责漏洞扫描

安全合规工程师

- 负责安全制度建设
- 负责安全意识培训
- 负责安全合规认证

2.4 人员安全管理

根据ISMS要求，销售易建立了自己的人员安全管理体系，包括入职前、任用中、调岗和离职管理。

入职前

员工在入职之前，销售易在法律法规允许的情况下，通过背景调查来确保入职员工符合公司的行为准则、保密规定、商业道德和信息安全政策。背景调查涉及刑事、职业履历和信息安全等方面，背景调查的程度取决于岗位需求。

任职中

员工在入职后，所有的员工必须签署保密协议，确认收到并遵守销售易公司的安全政策和保密要求，尤其关于客户信息和数据的机密性要求将在入职培训过程中被重点强调。所有新入职员工都必须参与信息安全意识培训和考核，销售易还会通过年度培训的方式（如安全意识周）来持续加强和提升全员的信息安全风险意识。

销售易依据员工的工作角色进行额外信息安全培训，确保员工管理的用户数据必须按照安全策略执行。

销售易通过企业价值观考核的方式检验每位员工是否以诚信、敬业的态度来管理每位客户的云端数据，保证其对客户、合作伙伴和竞争对手的尊重。

离职和调岗

员工离职需通过流程审批，管控环节包括工作文档交接，应用系统及邮箱帐号权限回收，VPN及网络访问帐号回收，公司电脑回收及门禁卡收回等。

员工如果涉及调岗，则其原有业务系统的权限会被回收，需要根据当前岗位需求重新申请。

三 安全防护

3.1 物理安全防护

销售易的系统均部署在如腾讯云、AWS（中国区）等业界知名公有云上，所在数据中心都有充分的物理安全监控和管控措施，并且均通过等保三级和ISO27001等安全认证。

3.2 网络安全防护

网络链路高可用性

采用多链路多ISP网络供应商接入服务，保障网络链路的高可用性。

网络抗击DDOS防护

采用云端的ELB机制，对外提供一个动态IP地址池，无论攻击者针对域名还是针对IP发起DDOS攻击，ELB机制都可以有效进行防御。

虚拟内网隔离

销售易生产系统通过VPC（虚拟私有网络）与外界网络隔离，并在VPC中划分公有子网和私有子网，不同的子网有不同的安全访问策略与限制。

网络访问控制

- 公司的各类服务，只有在经过安全团队审核之后，才能发布上线并对公众服务
- 高危端口和服务禁止对互联网开放，目前只对外开放了服务端口
- 内部后台应用仅对办公网开放
- 不同子网及子网内不同主机分别通过ACL映射、同时启用iptables防火墙进行不同粒度的访问控制，来保障安全限制无死角。

3.3 主机安全防护

系统软件安全配置标准

线上服务运行在可信的操作系统版本上，安装软件必须由运维人员从公司系统团队维护的可信安装源下载和安装。对于通用的系统软件，例如tomcat、nginx、ssh等，制定了对应的安全配置规范。通过主机安全防护产品实时采集服务器上运行的软件版本和配置信息，并进行相应的维护。安全团队也会跟踪业界安全问题，评估服务器上的软件是否有安全漏洞。一旦有安全漏洞产生，会通过应急响应流程推动基础软件的漏洞修复。

系统登录授权访问

服务器上的帐号依据权限大小进行划分，除了线上运维人员可拥有较高权限的用户组外，线上服务仅以低权限用户运行。

运维人员登录服务器时使用个人帐号体系，登录服务器的密码强制定期修改且有复杂度要求。运维人员登录服务器前，需要先提交权限申请，访问权限有时间控制。在通过审批后，才能获得对应服务器的登录权限。运维人员离职、岗位发生变动、申请的权限到期时，都会在对应的服务器上删除对应的帐号。

堡垒主机

对于生产服务器，运维人员需要先登录堡垒机之后，才能登录其他生产服务器。堡垒机只对特定的办公网段开放，并部署有操作日志记录和审计系统。

3.4 应用安全防护

访问控制

销售易提供以下多种机制共同保证只有数据的拥有者或得到拥有者的授权才能对数据拥有访问权限，包括：

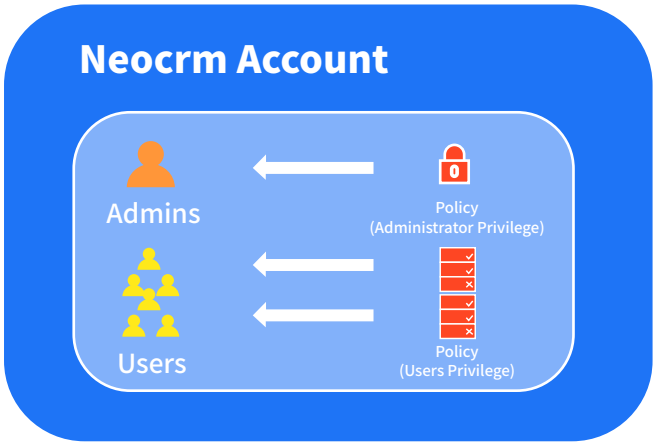
- Identity and Access Management (IAM) Policies
- Access Control Lists(ACLS)
- Bucket Policies

Type of Access Control	Account-Level Control?	User-level Control?
IAM Polices	No	Yes
ACLS	Yes	No
Bucket Polices	Yes	Yes

- 以上各种策略，可以精细地控制各种应用场景下数据的访问授权。

销售易系统充分利用了云存储的优势对整个系统做了全面容灾设计。同时严格定义了各用户的权限，保证每个用户仅有权限访问其使用到文件，无权浏览不应访问的文件。比如，内部员工未经授权，没有权限查看用户的文件。

销售易系统提供IAM管理机制，同一帐户下可以划分多个用户，每个用户可以精细粒度的控制用户的访问权限，可以满足各种安全需要，非常便于帐户权限的控制。



销售易建议用户严格定义内部使用人员的角色，对不同角色的人员提供不同的权限。比如管理员、开发人员、测试人员及运维人员，根据最小权限原则，严格定义不同人员的权限。

账号安全

账号安全体系依托口令策略和访问控制策略，禁用弱口令，监控非法

登录尝试。销售易给出上次登录的设备和时间、地点，以帮助用户识别是否正常登录。同时，通过账号监测平台，对用户同设备批量尝试登录账号进行监控报警，发现攻击行为，可将该设备拉至黑名单。此外，还提供用户双因素认证、并发登录限制、设备绑定、登录IP限制等功能来全方面保障用户的账号安全。

用户可以自行定制密码安全规则，包括如下可配置项：

- 密码有效期
- 密码历史
- 最小密码长度
- 字符要求
- 密码输入错误次数

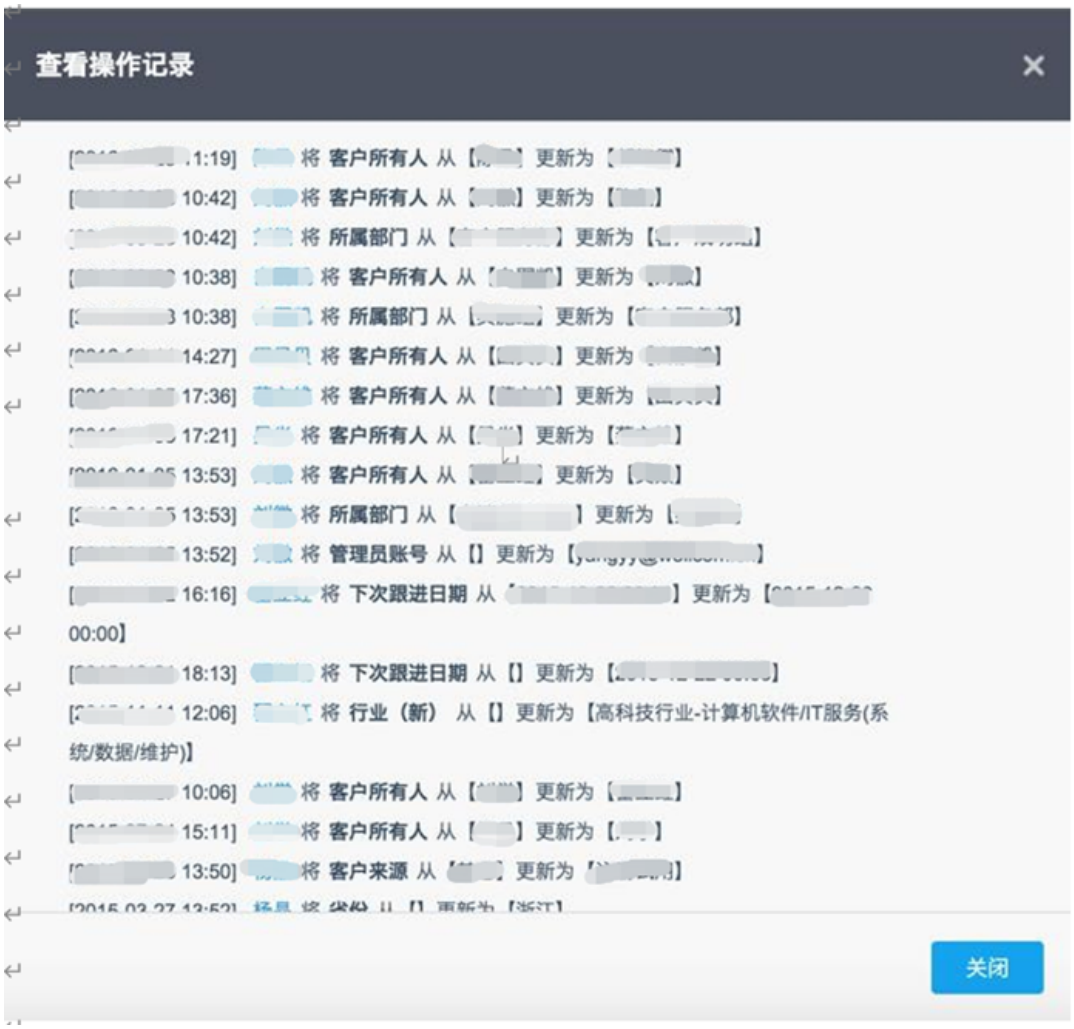
暴力破解&撞库防护

销售易账号基于可信设备判断是否进行二次验证，同时基于后端风控体系，实时监测账号破解、撞库与刷库等攻击行为，处理告警通知并处置恶意请求；账号依据信息安全风险库检测账号是否存在风险，发现存在风险的账号及时告知用户进行账号密码的修改。

安全审计

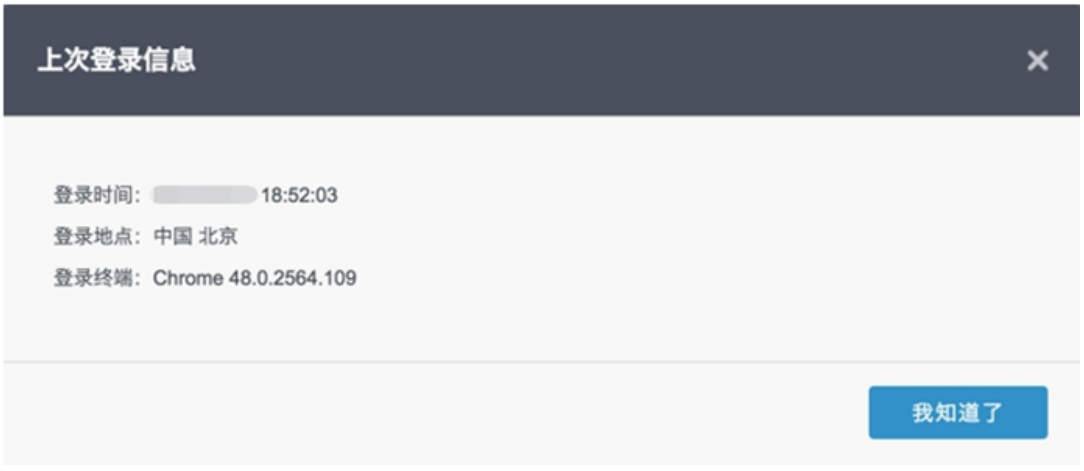
用户操作日志

销售易详细记录了用户的操作日志，用以监控和约束用户的行为操作。用户操作日志保存时间长达5年，以保证恶意操作的不可抵赖性。



用户登录日志

销售易详细记录了用户的登录日志，用户可以查看上次登录的时间、地点和登录终端。登录日志让用户可以方便发现异常登录情况，保障数据安全。



管理员操作日志

销售易提供详细的管理员操作日志，以记录系统的用户配置、权限配置等信息，以保证租户内部权限的安全和操作的不可抵赖性。

数据导入导出日志

销售易提供详细的数据导入导出日志，以记录用户对业务敏感数据的导入、特别是导出行为，以便在发生数据泄露的情况下帮助溯源和责任人定位。

WAF（Web应用防火墙）

销售易使用WAF对DDOS攻击，以及SQL注入、XSS、命令注入等OWASP TOP10的常见攻击手段进行严格地检查和过滤。

协议安全

基于SSL、TLS协议为应用程序提供数据保密性和完整性的基础上，销售易构建了一套完整的私有安全通信协议，通过加密用户在网络传输中的信息防止窃听，以确保信息在网络中传输安全。

企业通讯录安全

企业通讯录采用加密存储，可分级管理通讯录，针对不同人群设置不同权限；同时企业可以设置对重要部门进行保护，该部门的信息会自动隐藏，即使是企业内的员工，没有相应权限也无法访问。

当员工离职后会被自动移出对应的企业群，删除员工在该企业的权限。

企业可以设置对员工的手机号进行隐私保护，在对外展示员工信息时隐藏手机号码，防止信息泄露，但不影响销售易电话通讯和电话会议等相关功能的使用

客户端加密

销售易客户端的数据库进行了整库加密存储，根据用户设备信息通过加密算法生成的唯一密钥，保护用户客户端存储的敏感信息不被攻击者非法获取，保障用户的隐私数据不被泄露。

3.5 数据安全防护

依据数据安全生命周期，销售易从数据传输、存储、访问至销毁，使用了数据分级、数据加密等措施，保障了数据的保密性、完整性、可用性、真实性、授权、认证和不可抵赖性。

1. 传输安全

所有公网数据均使用业界认可的HTTPS、TLS安全协议传输，可以保证数据在公网传输过程中的保密性、完整性。

2. 存储安全

销售易凭借以数据为中心的安全愿景，将安全技术嵌入至整个数据安全生命周期中，对数据的存储有严格的安全要求，所有业务级别数据（包括客户端数据）均使用加密处理或密码保护来保障数据安全。

3. 访问安全

销售易为用户和企业数据提供访问控制保障。通过访问IP限制、细粒度的权限管控、数字水印、数据导入导出日志为人员的数据访问安全提供全面的防护和保障。

此外，只有特殊情况下（如需要解决技术问题）用户可以临时授权销售易技术人员进行远程登录协助，并且该授权可以随时取消或设置自动取消时间。

4. 数据销毁

若用户购买的销售易产品服务到期60天不再复用，销售易将注销该企业账户，并安全、彻底地删除掉所有相应数据以确保用户数据安全，完成数据生命周期管理。

5. 数据保障

销售易系统使用了云服务商中对象存储和云数据库两种数据存储服务。

对象存储作为文件存储服务，采用加密且多副本冗余设计，公有云服务商均承诺可保障99.99% 的可用性和 99.999999999% 的持久性。

云数据库作为数据存储服务，实现多数据中心主从实时同步并保证每个数据中心多副本，既满足服务的高可用性，又保证了实时备份。同时作为增强的数据备份方案，云数据库中的数据每天定时全量导出上传到对象存储服务中。

销售易所有与数据相关的服务器在云端上都做了定期的镜像拷贝存储在对象存储中来进行保障。

四 安全监控

4.1 应用监控

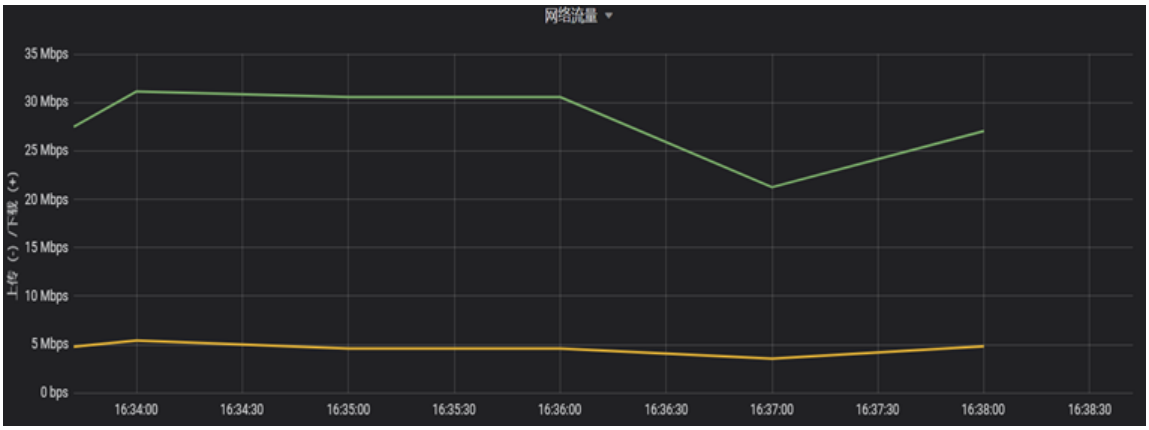
WAF（Web应用防火墙），可以实时地对应用系统入侵、SQL注入攻击、XSS攻击、命令注入攻击等行为进行监控和报警。

网站安全实时监控，采用市场成熟网站安全监控解决方案，实时对网站发生的安全威胁进行监控，一旦发现网站安全漏洞或风险可以实时提供报警服务，并且定期提供报表，对网站的安全监控历史数据进行分析。

销售易Web安全监控

4.2 网络监控

网络层级同时使用内部监控系统与第三方服务监控外网访问性能与连接状态。



销售易网络监控

4.3 主机监控

销售易系统均部署了功能全面的主机安全监控产品，包含多种功能：

资产清点

- 细粒度梳理关键资产
- 业务应用自动识别
- 与风险和入侵全面关联

风险发现

- 风险预览
- 安全补丁
- 漏洞检测
- 弱密码
- 应用风险
- 系统风险
- 账号风险

入侵检测

- 暴力破解
- 异常登录
- 反弹shell
- 本地提权
- 后门检测
- Web后门

合规基线

- 等保、CIS等多重标准
- 自动识别安全检查基线
- 一键任务化检测
- 自定义基线检查

销售易主机安全监控

4.4 数据监控

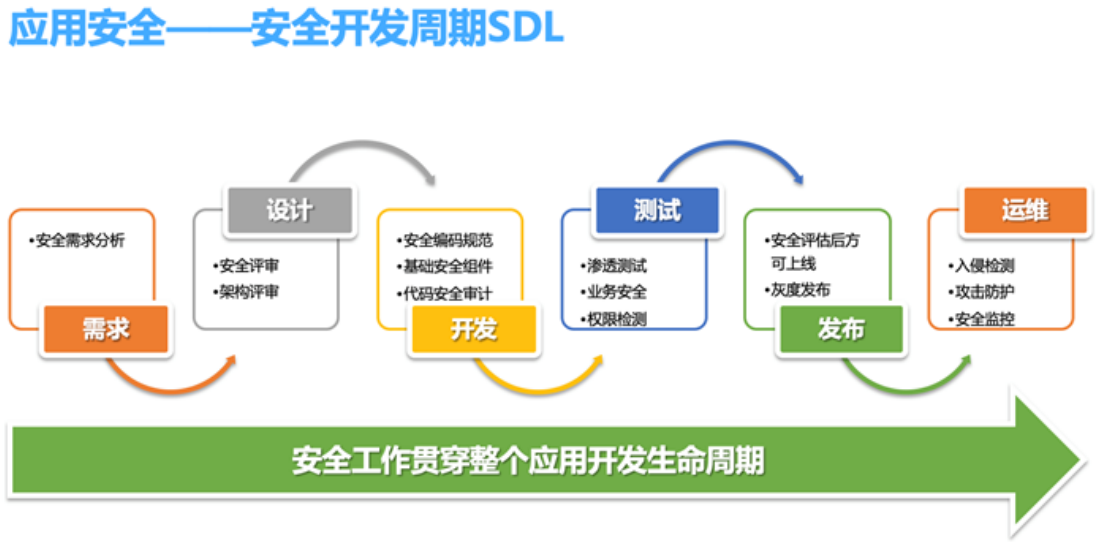
云端的安全审计覆盖所有数据活动的详细跟踪记录，并进行实时语境分析和行为过滤，从而实现对用户访问行为的主动控制，生成审计员所需要的信息。生成的结果报表使所有数据活动详细可见，如登录失败、权限升级、计划变更、非法访问、敏感数据访问等，这些行为是否合规一览无余，做到所有用户操作有踪可寻。

五 安全运行

5.1 安全开发

■ 销售易SDL

销售易产品在项目开发流程中引入了SDL(Security Development Lifecycle)，借鉴了微软推广SDL的经验，并结合企业级安全需求以及销售易自身的项目开发流程，控制项目整体的安全风险。SDL如下：



SDL建立

(1) 人员培训环节：安全工程师给开发人员进行安全开发规范、安全意识培训等，提高其安全意识。

(2) 安全需求分析环节：根据功能需求文档进行安全需求分析，针对业务内容、业务流程、技术框架进行沟通，形成相应安全Story以驱动安全开发。

(3) 安全开发环节：根据不同的开发框架开发安全包、提供安全编码规范及安全框架配置规范，避免开发人员写出不安全的代码。

(4) 安全测试环节：通过代码扫描工具进行白盒、黑盒扫描，并结合人工审核代码漏洞。

(5) 项目发布环节：安全部门依据上述环节评价结果决定项目是否发布。

(6) 安全运营与应急响应：安全工程师通过应急响应平台进行安全运营及事件应急响应。

■ 定期内外部渗透测试

销售易每年聘请外部专业安全公司，组织两次针对应用系统的渗透测试，及时发现并修复应用层面的安全漏洞。

另外，销售易安全部每年还会定期进行内部的白盒测试，从不同角度去发现、修复应用层面、代码层面的威胁。

■ 第三方组件安全

销售易使用基于业界知名开源软件搭建了SCA（软件组成分析）平台，并定期对应用系统使用的第三方组件进行全面细致地分析，从而发现存在高危风险的第三方组件并推动修复。

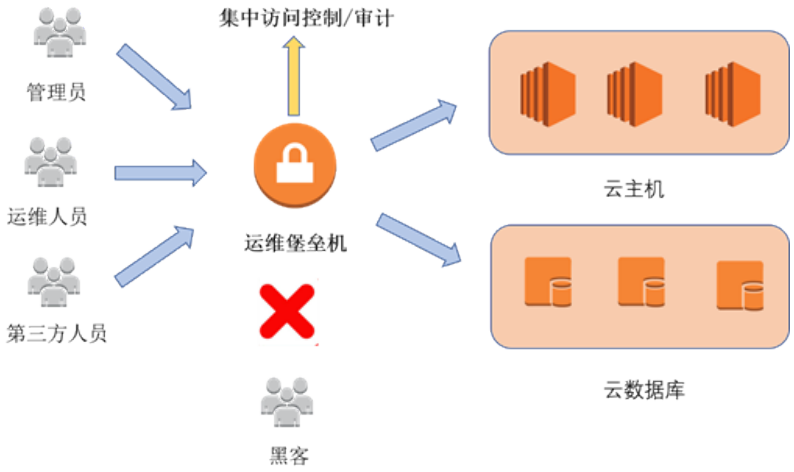
5.2 安全运维

■ 完善的运维流程

销售易根据ISO20000服务体系，建立了一套完善的运维服务流程，包括事件管理流程、服务请求管理、问题管理、变更管理流程、配置管理、发布管理等。

■ 可审计的运维操作

所有的运维操作必须通过运维堡垒主机认证、授权以及审计，所有操作都可审计查询。



■ 可信的运维地址

针对可以访问生产系统的运维IP地址范围，在云端使用了ACL控制手段，目前能访问生产系统的只有销售易的办公网段。

■ 加密的运维数据传输

目前所有的运维操作均使用SSH（V2）版本的加密协议，防止敏感信息在互联网传输被窃取。

5.3 符合性管理

销售易根据国家信息安全《中华人民共和国网络安全法》《等级保护基本要求》、ISO27001、ISO20000、ISO27701等国内与国际相关法律、法规要求，设置与信息安全监控机构之间的联络员，制定实施程序，以确保提供的销售易产品符合国家关于知识产权相关法律和法规要求。

销售易同所有企业及开发者签署保密协议，并通过定期检查识别、记录、评审保密协议中数据安全的相关控制要求（如访问控制、防泄露及完整性要求），防止不正当披露、篡改和破坏数据。

六 安全运行

6.1 安全事件管理

销售易制定了完善的信息安全事件管理规范和处理，对信息安全事件分类、信息安全事件分级、信息安全事件报告及处理、信息安全事件的处理和解决、信息安全事件的反馈和关闭、信息安全事件的通报、信息安全事件回顾和分析做出了明确定义。

6.2 安全通报机制

在信息安全事件管理规范中明确了安全通报的流程、触发机制、根据安全事件的分级分别启用相应级别的安全通报机制。

6.3 应急处理机制

销售易制定了一套完善且适用于自身业务的通用应急预案及专项应急预案，成立了自己的应急响应团队（由公司高管、运维部、安全部组成），规范了应急处理的流程，并且每年启动一次应急预案的演练。

6.4 业务连续性管理

销售易能够应对线上各类风险，具有自动调整和快速反应的能力，保障销售易业务连续运转。销售易通过了ISO20000认证，以国际安全认证标准保障服务的连续性，服务可用性可达99.9%。

销售易的灾难恢复机制，建立在公有云提供的服务基础上，主要包含以下方面：

1.备份机制

系统环境：销售易通过快照的方式保存在对象存储上，供快速扩展和环境恢复。

数据信息：一方面每日定时快照到对象存储上，另一方面利用云数据库的跨AZ（多个数据中心）同步机制，共同保障数据的安全和完整。

系统代码：销售易采取本地备份和云端对象存储双备份机制。

可靠性：销售易依据云服务商的服务承诺，可保障11个9的可靠性，并采用对象存储多副本冗余设计以保障系统的整体可靠性。

2.恢复机制

系统环境：根据对象存储上的快照机制可以迅速恢复服务机器。

数据信息：根据云数据库的跨AZ（多个数据中心）同步机制，若需要恢复或调整，则使另一数据中心的副本自动升级为主实例即可，并且可以保证数据完全一致。如果实时切换失效，还可以根据对象存储上的每日定时快照，恢复数据到前一天。

系统代码：从对象存储上下载并自动化部署到新的机器上。

可靠性：根据公有云的服务承诺，其多个数据库中心的设计可以保证任何时候都能启动机器进行恢复操作。

七 品牌价值

7.1 安全认证

销售易通过了ISO20000 IT服务管理体系、ISO27001信息安全管理体系、ISO 27701隐私信息管理体系、国家等级保护三级认证等国际和国内认证，证明销售易的生产系统已经达到国际、国内领先的安全水平。同时，销售易的系统获得了“网站安全性证明”。

7.2 进一步了解

如果您想进一步了解销售易安全的整体情况，可以访问以下网址

官网安全版块：

此外，关于信息安全方面的更多文档和资源，请访问以下网址

隐私白皮书：

销售易安全最佳实践指导手册：

Neocrm 销售易

www.xiaoshouyi.com

销售易公众号

销售易视频号