阿里巴巴钉钉安全白皮书 V1.0

目录

前言

钉钉是阿里巴巴集团自主创新,面向企业级的 SAAS 平台，基于阿里巴巴集团十多年安全技术研究积累的成果，打造了业界一流的安全保障体系、高可靠的系统实现机制，为企业信息安全提供全方位的安全保障！

术语定义

SDL： Security Development Lifecycle 的简称，安全开发生命周期；

撞库：撞库是黑客通过收集互联网已泄露的账户和密码信息，生成对应的字典表，尝试批量登陆网站后，得到一系列可以登录的账户；

DDOS 攻击： 分布式拒绝服务(DDoS:Distributed Denial of Service)攻击指借助于 C/S 技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动流量攻击，造成目标的业务系统无法提供服务；

一. 组织安全

钉钉安全团队由安全管理委员会、信息安全、安全审计、物理安全团队组成，通过高效、协同的工作给广大用户提供稳定、健康、安全的工作环境。

1.1 安全管理委员会

安全管理委员会成员由集团 CRO、安全团队负责人、产品负责人及技术负责人组成，监督并决策信息安全体系的建设，对钉钉业务整体安全负责。

1.2 信息安全团队

信息安全团队由应用安全、系统&网络安全、安全开发专家组成，信息安全团队负责产品安全架构及安全运营工作，是钉钉信息安全体系的建设者，在安全策略、安全开发流程设计、落实及执行中扮演重要的角色。

1）设计、开发和运营入侵检测、攻击防护产品，提供 7*24 小时安全监控，动态联动防攻击产品.如: Aliguard DDOS 防御系统、漏洞扫描与检测等；

2）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;

3) 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;

4）通过安全解决方案流程，在产品设计阶段，对功能需求进行安全评审，在产品发布前，进行安全测试以及产品发布后，进行安全回归测试，以保障钉钉业务的安全运营；

5) 借助公司的人才资源及技术沉淀，定期对钉钉内部和外部应用进行漏洞检测与扫描，及时发现安全漏洞，并在预期时间内完成漏洞修复；

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) 定期进行攻防演练，评估安全策略可靠性和控制措施的适用性;

8) 定期为钉钉员工提供安全意识培训,包括个人准则、信息保护、数据安全认证和安全开发等领域;

9) 积极参予安全论坛与会议，吸取业界前沿的安全技术并保持与外部安全专家、白帽子黑客的交流沟通;

1.3 安全审计团队

安全审计团队主要对钉钉系统化的监测、控制、处理、独立审查，以验证是否满足信息安全体系及标准，通过审计以满足合规性要求，如 GB/T 22080-2008/ISO/IEC 27001:2005、《信息系统安全等级保护基本要求》等。

1.4 物理安全团队

物理安全团队主要根据机房安全相关的国家标准：GB/T2887－2000:《计算机场地通用规范》、GB 50174－93：《电子计算机机房设计规范》国家标准；GB 9361－88：《计算站场地安全要求》保障钉钉数据中心基础设施的高安全性。

二. 合规安全

2.1 安全体系

1）ISO/IEC 27002，推动信息安全体系(ISMS)建立与实施，采用以风险管理为核心的方法管理公司和用户信息，保障信息的保密性、完整性及可用性；安全审计团队依据该安全标准，审核钉钉技术方案与技术框架内部信息安全管理同国际信息安全最佳实践接轨。

2）等级保护基本要求：根据国家下发的《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》开展信息安全等级保护工作，主要是指对国家、法人和其他组织及公民的专有信息，公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应与处置。

2.2 政策合规

钉钉根据国家信息安全相关法律、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，以确保提供的钉钉产品符合国家关于知识产权相关法律和法规要求。

钉钉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。

三. 人员安全

3.1 尽职调查

在入职前，阿里巴巴在国家法律法规允许的情况下,通过一系列背景调查手段来确保入职的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,背景调查手段涉及刑事、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。

3.2 安全生产

在入职后,所有的员工必须签署保密协议,确认收到并遵守阿里巴巴集团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。此外,阿里巴巴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。最后,阿里巴巴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;阿里巴巴提供机密报告机制以确保员工可以匿名报告任何违反安全政策、商业道德的事件.

四. 数据安全

信息安全主要目标之一是保护业务系统和应用程序的基础数据安全。依据数据安全生命周期，钉钉从数据创建、存储、使用、共享、归档至销毁，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。

4.1 数据分级

钉钉对所有用户和企业数据提供存储安全保护;根据存储与使用的数据，实施数据等级保护策略，按照数据价值和敏感度对数据进行等级划分，根据数据安全分级，有对应的保护策略和要求，对用户和企业数据进行安全存储与保护。

4.2 数据安全与加密方案

钉钉凭借以数据为中心的安全愿景，通过数据分类分级、数据加密和密钥管理为敏感数据提供可持续的信息保护，实现数据的灵活性、可靠性和可管理性；借助密钥管理中心和加解密产品实现数据安全保护和控制，将安全技术嵌入至整个数据安全生命周期中，以保障数据安全属性。

4.3 密钥管理中心

密匙管理中心(KeyCenter)是阿里巴巴集团内部唯一的密钥管理系统，为众多核心业务提供密匙管理服务。其主要负责密钥的存储、使用、分发、更新等，并提供数据加解密及业务级别敏感数据保护。它的设计与管理满足行业合规性及审计要求。

4.4 数据访问及用户授权第三方应用访问其敏感信息

钉钉为用户和企业数据提供访问控制保障。所有产品使用的数据，用户隐私或机密数据严格控制权限申请，数据加密存储；第三方应用访问与使用用户或企业数据，必需经过企业、用户可感知的授权。

4.5 数据使用与防爬

钉钉根据用户和企业数据进行了等级保护，对用户使用和应用展示进行了严格控制，禁止展示机密信息及未脱敏信息，同时对于需要展示信息的场景,使用了防爬安全产品，阻断对敏感信息的爬取。

4.6 数据安全审计

安全审计覆盖所有数据活动的详细跟踪记录，并进行实时的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并做到所有用户操作有踪可寻。

4.7 数据销毁管理

所有存储数据的存储介质(如硬盘等)，如若需要维修必需先进行卸载；需要报废或移出数据中心的网络设备及存储设备，依据 DoD 5220.22-M、NIST 800-88 标准进行清除数据、磁盘消磁以及物理销毁。

五．应用安全

5.1 钉钉 SDL

钉钉产品在项目开发流程中引入了 SDL，借鉴了微软推广 SDL 的经验，并结合企业级安全需求以及钉钉自身的项目开发流程，控制项目整体的安全风险。SDL 如下图 1

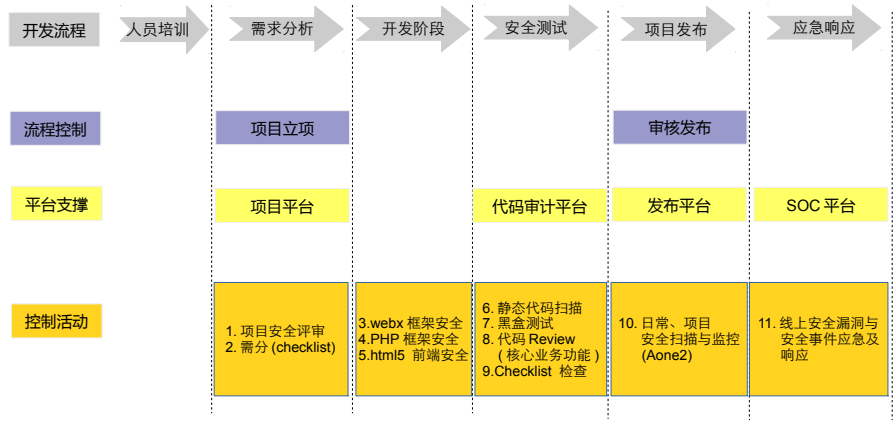

图 1 SDL 流程图

安全开发流程参照软件安全开发周期（SecurityDevelopmentLifecycle）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）安全需分环节：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《安全需求分析建议》；
（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；

（5） 安全测试环节：通过阿里自主研发的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；

（6） 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；

（7） 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；

5.2 业务安全

5.2.1 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。对非常用设备的登陆，需用户进行密码+动态口令登录的双因素验证。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。

除已有的风控体系外，也会提供相应的安全辅助功能，如二次验证、双因素认证、指纹验证等方式，给用户账号安全保障提供更多维度的选择。

5.2.2 暴力破解&撞库

钉钉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，告警通知及处置恶意请求；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，进行账号密码的升级。

5.3 钉钉基础与特色安全

5.3.1 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，钉钉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。

5.3.2 企业通讯录

企业通信录采用加密存储，可分级管理通信录，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，没有相应权限无法访问。

对于不同公司的信息，存储空间是相互隔离的，当员工离职后，会被踢出对应的企业群，自动剥离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，但不影响钉钉电话通讯和电话会议等相关功能的使用。

5.3.3 企业云盘

5.3.3.1 云盘访问控制

钉钉企业云盘具备独立的访问控制鉴权功能，对于用户通过点对点或群组的方式上传的文件，访问控制的粒度会细化到个人或企业，其他人在非授权情况下无法访问或下载文件。

保存到云盘的企业文件具有企业权限保证，即使被转发给非本企业的用户，对方也无法查看该文件；聊天会话中传输的文件也有相应的权限保证，只有参与该聊天的人能够查看对应文件，不在此聊天会话中的人无权查看文件。

钉钉企业通过这一系列措施保障企业文件存储、传输和访问的安全。

5.3.3.2 传输与存储安全

企业云盘为保障用户数据安全，会对所有上传数据进行分片以及采用 SSL/TLS 加密传输，并且在云端应用物理隔离和分片存储双重保护手段，在确保速率的同时保障云盘数据存储安全。

5.3.4 企业云邮箱

5.3.4.1 企业邮箱安全策略

钉钉企业邮箱以生产数据不出生产集群为中心思想，基于阿里巴巴集团十多年信息安全风险管控经验，以保护数据的机密性、完整性、可用性为目标，根据不同类别数据不同的安全级别，分别进行安全管理和技术控制措施的设计，并在执行过程中对其进行复查和改进，最终制定了一系列防范数据泄露、篡改、丢失等安全威胁的管控方案。

5.3.4.2 企业邮箱反垃圾体系

钉钉企业邮箱的反垃圾体系基于云计算平台的高性能反垃圾系统，该系统作用于云邮箱诸多模块的边界，能从行为和内容等多纬度对垃圾邮件进行识别和阻拦，从而保证企业邮箱不被垃圾邮件干扰。

该系统的主要功能包括攻击防护/异常检测、身份识别、内容/行为检测以及智能纠错四大部分，每个类别又设置了多层过滤检测网，从而为企业邮箱提供高效的反垃圾、反病毒能力，确保企业邮箱的安全。

反垃圾防护体系架构如下图 2：

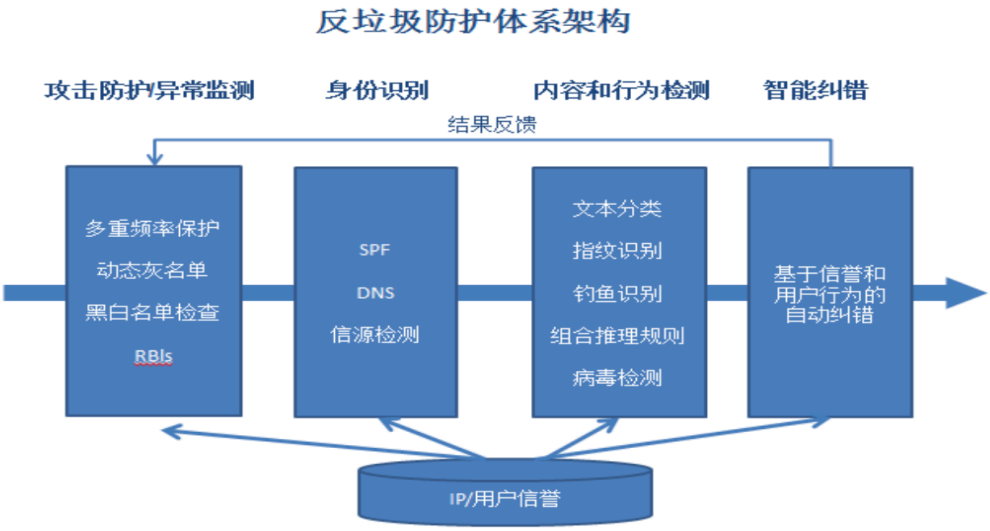

图 2 反垃圾防护体系

功能亮点和优势：

1.海量数据挖掘：基于蜜罐和用户反馈建立邮件特征模型库。邮件特征是区分正常和垃圾邮件的基础，特征的识别和提取能力在一定程度上决定了系统的反垃圾能力，云邮箱的反垃圾系统除了采集来自垃圾邮件本身的特征，还同时采集和综合运用来自互联网的垃圾网页特征，建立起强大的特征模型库。由于很多垃圾邮件（特别是钓鱼邮件）都与诸多垃圾网站有着千丝万缕的关系，引入这些特征提高了反垃圾系统的对垃圾邮件的识别能力；

2.快速响应的组合规则引擎：各式各样的垃圾邮件层出不穷，如何快速应对新暴发的垃圾邮件是一个难题，云邮箱反垃圾系统开发出灵活强大的组合规则引擎，无需后续额外的程序开发，便能针对新的垃圾邮件类型快速定义反垃圾策略，作出迅速的防御措施；

3.基于 IP 和用户信誉的智能纠错系统：云邮箱的反垃圾系统特别设置了基于 IP 和用户信誉的纠错环节，以减少其它自动化策略可能带来的漏判和误判；

4.针对钓鱼和欺诈邮件的专项检测机制：除了一般的垃圾邮件，对用户危害更大的是钓鱼和欺诈性垃圾邮件，经过深入的分析研究钓鱼和欺诈邮件的内容和行为特征，制定了钉钉特有的反钓鱼库，构建了针对钓鱼/欺诈邮件的专项检测机制；

5.邮件指纹系统：区分相似邮件的利器。

5.3.4.3 登陆日志自助查询

在网页版邮箱上，用户可以方便的自助查询自己的历史登录日志，如果自己的邮箱存在异常登录情况，用户可以轻易地主动发现，具体示例如下图 3：

79	2014年10月21日 18:30	未知	41.82.30.117	个人邮箱	成功
80	2014年10月21日 18:14	未知	41.82.30.117	个人邮箱	成功
81	2014年10月21日 18:13	未知	41.82.30.117	个人邮箱	成功
82	2014年10月21日 15:28	江西省 南昌市	59.53.173.220	个人邮箱	成功
83	2014年10月21日 15:26	江西省 南昌市	59.53.173.220	个人邮箱	成功
84	2014年10月21日 13:43	台湾省	61.220.97.89	个人邮箱	成功
85	2014年10月21日 08:51	江西省 南昌市	59.53.173.220	个人邮箱	成功

图 3 异常日志查询

5.3.4.4 数据备份

钉钉企业邮箱数据备份具备自动化、永远在线、热备份的特点。

5.3.5 特色安全功能

5.3.5.1 可信设备

钉钉会对所有登录的用户进行设备认证，如果该设备没有通过认证则不允许登录；可信设备认证需要经过账号或密码及验证码的认证；Web 设备的验证需要手机端进行辅助。

5.3.5.2 客户端加密

钉钉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。

六. 系统&网络安全

6.1 系统安全

6.1.1 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，必须由运维人员从集团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，通过基线系统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。

6.1.2 系统登录授权访问

服务器上的帐号依据权限大小，分为高中低三个用户组，除了线上运维人员可拥有较高权限的用户组外，普通员工只能申请低权限的用户组，线上服务也以低权限用户运行。

员工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。员工登录服务器前，需要先提交权限申请，访问权限有时间控制。在通过审批后，员工才能获得对应服务器的登录权限。员工离职/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。

对于生产服务器，员工需要先登录经过堡垒机之后，才能登录其他生产服务器。堡垒机经过了特别的加固，只对办公网开放，启用了双因子验证，并部署有操作日志记录和审计系统，堡垒机上的操作会被实时传送到远端进行存储和审计。

6.1.3 系统安全检测防御产品

集团的服务器上统一部署了自主研发的主机端安全产品，并依托大数据处理平台 ODPS，对恶意流量进行分析，实现对入侵等安全事件的检测。

6.2 网络安全

6.2.1 安全域划分

集团的网络依据用途划分成办公/测试，生产，公有云等多个安全域，对于不同的安全域之间，除了部分经过安全加固的可信中间程序外，相互之间不能互访。

6.2.2 网络访问控制

集团的各类服务，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。内部后台应用仅对办公网开放。

另外，安全团队会通过自主研发的“探照灯”系统，定时地依据 acl 规则进行白盒审计，依据端口扫描进行黑盒审计，用于主动及时发现访问控制中存在的安全问题。

6.2.3 流量劫持

针对 http 协议在网络传输过程中，可能会被篡改/窃听/截取，为了防止用户的隐私数据在传输过程中被窃听或者泄露，集团的重要业务都已经启用 https 协议来代替 http 协议。

对于 DNS 劫持，集团的 DNS 团队通过多种手段在全国范围内监控重要域名的解析结果，一旦发现有严重的 DNS 劫持，有专业的安全工程师快速响应。

6.2.4 DDoS 安全防御

6.2.4.1 网络层攻击防御

钉钉数据中心主骨网入口，自建流量清洗中心，DDoS 清洗中心抵御各类基于网络层、传输层的 DDoS 攻击（包括 SYN Flood、UDP Flood、UDP DNS Query Flood、(M)Stream Flood、ICMP Flood 等所有 DDoS 攻击方式），并通过安全运营后台实时掌握网络攻击趋势及防御状态。

6.2.4.2 七层攻击防御

钉钉业务系统统一部署了阿里安全团队研发的应用层攻击防御产品(TMD),主要用于检测与防护 CC 攻击,防御规则可根据业务自由定制,安全工程师通过安全运营后台实时掌握应攻击与防御情况。

七. 物理与环境安全

7.1.物理安全

钉钉数据中心包含以下标准的物理安全控制要求：

（1） 数据中心各线上设备区域系统、各核心骨干区域系统、各动力区域系统、各仓储系统、各报警监控系统的访问均需使用定制的电子卡，且电子卡由数据中心专门物业保管，特定授权需求方按需求领取归还，并配备紧急电子卡以备不时之需（如常规电子卡遗失），一旦发生遗失情况立即申请电子卡管理系统进行权限注销；

（2） 数据中心的物理设备（包括其对应的各种组件），配件耗材的安置或存放区域必须要与所有办公区域和公共区域隔离（如办公室或大堂）；

（3） 数据中心所有钉钉专属物理设备、设备配件、网络耗材，以及设备厂商的维修设备、配件、耗材等进出数据中心，必须由钉钉内部授权人员发送盖有专人保管印章的设备进出单传真，数据中心现场核实无误后方可允许设备、配件、耗材等的进出；

（4） 仓储系统中的重要配件，如核心网络设备的网络模块，精密存储介质等，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；

（5） 仓储系统中的任何配件，必须由授权工单和授权人员方能领取，且领取必须在仓储管理系统中进行登记记录，数据中心管理有专人定期对所有仓储系统物资进行综合盘点追踪；

（6） 数据中心内部的每个区域，或外部走廊区域，或仓库门口区域，都使用了摄像机，物业保安 7x24 小时分段巡逻，并对所有基础设施进行 7x24 小时集中视频监控；

（7） 采用全方位电子摄像机对数据中心的基础设施内外部区域进行视频监控，对设施区域中的其他系统进行检测和监控跟踪访问人员情况；

（8） 所有人员活动记录电子保存（长期），所有视频记录被保存（3 个月），以备后期审计，同时提供额外的安全控制措施，如:特定区域采用隔离或生物识别技术认证；

（9） 只允许具备长期授权名单内的内部人员（实时更新），或审批通过的其他人员，以及授权认可的第三方固定人员名单内的人员（每月更新）进入数据中心，且非长期授权人员再以核实需求工单真实性的形式进行二次审核，准确无误后方可进入；

（10）非长期授权，非固定人员授权名单内的人员访问，必须要求数据中心内部管理需求方在流程系统上提交需求，由各层级主管提前审批通过后，方可同意其访问想要访问的内部特殊区域，并由对应数据中心的专人全程指导陪同。数据中心管理不定期对访问数据中心的人员登记情况进行审计，严格控制非授权人员访问数据中心；

7.2.环境控制

钉钉数据中心采用一系列措施来保障运行环境：

（1）电力：为保障数据业务 7*24 持续运行，数据中心采用冗余的电力系统（交流和高压直流），主电源和备用电源具备相同的供电能力，且主电源发生故障后（如电压不足、断电、过压、或电压抖动），会由备用发电机和带有冗余机制的电池组对设备进行供电，保障数据中心在一段时间的持续运行能力，这是钉钉数据中心一个关键的组成部分。

（2）气候和温度：均采用空调（新风系统冷却或水冷系统冷却）保障服务器或其他设备在一个恒温的环境下运行，并对数据中心的温湿度进行精密电子监控，一旦发生告警立即采取对应措施。并且，设备冷风区域进行了冷风通道密闭，充分提高制冷效率，绿色节能。空调机组均采用 N+1 的热备冗余模式（部分数据中心采用 N+2 的冷、热双重冗余模式），空调配电柜采用不同的双路电源模式，以应对其中一路市电电源发生故障后空调能正常接收供电。且在双路市电电源发生故障后，由柴油发电系统提供紧急电源，减少服务中断性的可能，以防止设备过热。

（3）火灾检测及消防：自动火灾检测和灭火设备防止破坏计算机硬件。火灾探测系统的传感器位于数据中心的天花板和底板下面，利用热、烟雾和水传感器实现。在火灾或烟雾事件触发时，在着火区提供声光报警。在整个数据中心，也安装手动灭火器。数据中心接受火灾预防及灭火演练培训，包括如何使用灭火器。

八. 灾难恢复与业务连续性

钉钉依托于淘宝、阿里云技术，能够应对线上各类风险，具有自动调整和快速反应的能力，保障钉钉业务连续运转。

8.1 应急与灾备技术

钉钉建立了本地应急系统及容灾系统，本地应急系统、容灾系统与生产系统相互配合共同保证整体业务连续性。

灾备采用双机房互备，数据库主备库热备，通过自动化运维平台，实时故障检测，切换无需人工干预，保障核心应用不中断，系统恢复方便快捷，可进行自动伸缩扩容，在突发事件及自然灾害时，为钉钉基础服务可用性及可持续服务提供保障能力。

8.2 应急与灾难恢复管理

钉钉建立了完备的应急响应及灾难恢复流程。应急响应组由安全专家、业务专家、技术专家组成，制定了完备的应急响应制度及灾难恢复流程，并定期组织灾备演习和维护。