飞书安全白皮书

版本（V 1.3）

飞书团队

版本变更记录

日期	版本	说明
2018年12月01日	V1.0	版本创建
2019年1月10日	V1.1	增加部分内容
2020年2月14日	V1.2	新增并修改部分内容
2020年9月15日	V1.3	新增并修改部分内容

前言 5
一. 安全团队及职能 5
二. 合规与隐私性 5
三. 人员安全 8
四. 客户端安全 8
4.1 运行环境安全 8
4.2 数据安全 9
4.3 安全漏洞防护 9
4.4 客户端安全策略 9
4.5 客户端数据安全方案 9
五. 网络安全 9
5.1 网络访问控制 9
5.2 DDoS及网络攻击防御 10
5.3 网络传输加密 10
六. 服务器安全 10
6.1 服务器访问控制 10
6.2 漏洞扫描 10
6.3 入侵检测 11
6.4 异常检测 11
七. 应用安全 11
7.1 安全开发流程 11
7.2 用户账号安全 12
7.3 漏洞与安全事件管理 12
八. 数据安全 13
8.1 数据传输 13
8.2 数据存储 13
8.3 数据访问 14

8.4 数据销毁 14

8.5 数据安全检测 15

九. 物理基础设施安全 15

9.1 物理访问授权 15

9.2 运营管理安全 15

十. 灾难恢复与业务连续性 16

10.1 备份与灾难恢复 16

10.2 业务连续性保障 16

10.3 应急演练 16

十一. 变更控制 16

11.1 程序变更 16

11.2 源代码控制 17

11.3 基础架构变更 17

11.4 变更监控 17

前言

北京飞书科技有限公司（“以下简称飞书科技”）提供的新一代企业办公套件SaaS云服务—飞书办公套件，以“移动友好、实时协作、统一入口”为特点，帮助企业提升工作效率，降低生产成本和管理成本，开启向更高效、更协同、更安全的智能化公司转变。公司使用信息技术和应用系统以支持与飞书办公套件之研发、运营等相关控制活动的有效开展。

飞书办公套件的功能包括即时通讯、云文档、云盘、智能日历、视频会议、开放平台、飞书招聘、飞书OKR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、用户数据进行全生命周期的安全保障。飞书产品的设计、开发和运营充分考虑了各国的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之国家用户对安全合规性、个人隐私性以及数据保护的法律法规和原则要求。

一. 安全团队及职能

飞书科技作为SaaS服务提供商，一直都把用户业务和数据的安全保护列为最高优先级工作。公司具有完善的基础架构安全以及用户业务、数据安全保护体系，可以为用户提供从物理到应用层面的全方位防护。

飞书科技的产品安全团队由安全管理与合规、业务安全、数据安全、应急响应、安全工具开发团队构成。工作内容包括产品设计安全评估、代码安全审阅、漏洞扫描、渗透测试、威胁情报、入侵检测、应急响应、数据安全、安全合规等。

二. 合规与隐私性

飞书科技高度重视产品的合规性，由安全与合规部专职负责，积极对标国内和国际最高标准合规性要求。目前飞书科技旗下多个产品已通过国家及国际的多项合规性认证， 包括公安部等级2.0保护三级、ISO27001、ISO27018、ISO27701、ISO22301等认证，完成了SOC 1 Type II、SOC 2 Type II 以及SOC 3服务鉴证报告。标志着我们在信息安全管

理、服务质量管理、IT服务管理等方面达到了更规范化、更标准化的水平，为公司全面质量体系的改进和完善奠定坚实的基础。

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。飞书科技的数据中心、管理体系、研发、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。

ISO27018 是首个专注于公有云中个人信息保护的国际认证标准，基于 ISO27002 信息安全管理实用规则，并针对适用于公有云个人可识别信息 （PII）的安全控制体系提供了实施指南。飞书通过此项认证，意味着我们在保护企业数据、保障用户个人信息安全、防止信息泄漏等方面已经达到了高标准的业界实践。

ISO27701是首个真正意义上构建出具有PDCA完整运行闭环的隐私信息管理体系标准。其详细规定了建立、实施、维护和不断改进隐私信息管理系统的各项要求，在信息安全保护的基础上将处理个人可识别信息 （PII）所需的隐私保护措施纳入考量。飞书获得此项认证，是对我们长期以来在隐私合规体系建设方面工作的充分肯定。

ISO 22301：2012是业务连续性管理（BCM）的国际标准，旨在帮助组织准备并确保其业务在面对自然灾害或信息安全漏洞等外部威胁时仍能够继续发展。采用业务连续性管理系统可以使组织做好业务弹性的准备，即使发生事件，也可以确保客户和利益相关者的连续运营。获得ISO 22301认证表明组织已制定了适当的人员和资源管理计划，准备应对业务威胁事件。

上述的四项ISO认证范围内的服务包括：

- 飞书办公套件服务：即时沟通，云文档，云盘，日历，音视频会议，开放平台
- 人力资源服务：飞书 OKR，飞书招聘

《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。飞书采用的是3级信息系统的保护策略，并通过了专业测评机构的测评。说明飞书产品在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。

系统及组织控制（SOC）报告是独立的第三方鉴证报告，是由专业的第三方会计师事务所依据美国注册会计师协会（AICPA）的相关准则出具的服务机构内部控制相关的系列报告。其中SOC 1是根据《鉴证业务准则公告》(SSAE 18）或《鉴证业务国际准则 第 3402 号》(ISAE 3402）评估组织内部控制措施的有效性，主要关注用户机构财务报告相关的内部控制活动，涵盖服务是飞书OKR；SOC2根据五项“信任服务原则”（安全性，可用性，处理完整性，机密性和隐私性）定义了管理客户数据的标准，涵盖的服务包括即时沟通、云文档、云盘、日历、音视频会议、开放平台、飞书OKR；SOC 3 报告是分发给公众的报告，涵盖的服务范围与SOC2报告相同。飞书产品会经过第三方的定期审核，以检验产品是否符合这项标准；此标志着我们拥有可靠的系统安全设计，可以安全地管理客户数据，保护组织的利益以及客户的隐私。

飞书科技积极跟进国内、国际对产品合规的要求，通过安全管理与合规团队对接各级监管机构，确保提供的产品和服务符合要求。

飞书科技有专门的隐私团队，对用户隐私协议、产品的隐私性保护设计、用户隐私数据的收集与使用进行审查，确保用户的隐私数据被妥善使用和处理，并且对用户保持合理的透明度。

三. 人员安全

飞书科技建立了安全的人力资源管理流程：

- 新员工的聘任须经过人力资源专员和岗位需求部门主管的审批，新员工招聘流程与结果记录在人力资源系统中；
- 新员工录用前，人力资源部会根据岗位的重要性，并在国家法律法规允许的情况下对员工进行背景调查，确保该员工的录用符合公司的各项规章制度；
- 新员工须签订劳动合同和保密协议，其中对员工在信息安全方面所应承担的责任和义务进行了规范；
- 法务部每年对员工保密协议和第三方保密协议的法律条款进行至少一次审阅并在需要时进行更新，更新后通过内部知识平台进行发布，以确保所有员工和相关人员可以获取最新的保密协议；
- 员工离职须由本人或部门领导在人力资源系统中发起申请，经过人力资源部、相关职能部门进行审核后方可正式离职。

飞书科技建立了完善的培训及学习体系，新员工入职后均须参加包括公司文化、规章制度、信息安全以及奖惩机制等内容的培训。同时，公司会不定期针对员工的专业知识技能和信息安全意识组织培训，建立了如下培训机制：

- 公司不定期组织信息安全相关培训，增强员工的信息安全技能；
- 公司不定期举行信息安全活动，对信息安全意识进行宣贯；
- 公司不定期通过多种方式向员工传达安全意识，如制作安全意识宣传资料并通过邮件、宣传画等形式传达至员工。
-

四. 客户端安全

4.1 运行环境安全

飞书科技的APP对运行的环境会进行严格的检测，包括root检测、越狱检测、调试检测、

注入检测等，检测目的是保证客户端运行在可信任的环境中，以防程序被破解或被恶意软件所利用。

4.2 数据安全

飞书科技的APP采用操作系统自带安全机制，进行APP之间的权限隔离。客户端本地信息均加密进行存储。客户端与服务器之间的全链路通信，均采用https或wss进行加密。

4.3 安全漏洞防护

飞书科技具有专职移动安全漏洞挖掘团队，对android, iOS, windows, macOS客户端进行安全评估和漏洞挖掘，同时对使用的第三方组件（库、SDK）进行漏洞检测，尽可能发现应用程序存在的漏洞，保证客户端的安全。

4.4 客户端安全策略

客户管理员可以通过管理控制台配置自定义安全策略，并应用到客户端。

4.5 客户端数据安全方案

飞书科技在Android客户端都集成了团队自研的数据安全方案，为客户端本地的隐私数据提供了系统级加密能力以及数据与设备的唯一绑定功能。即使攻击者窃取了用户加密的数据，也无法在自己的设备中解密使用。大范围增强了用户的数据安全边界，大幅度降低了用户数据泄露的几率。

五. 网络安全

5.1 网络访问控制

飞书科技使用公司自有设施提供基础架构服务，包括机房、传输、网络、服务器、操作系统等，并由其提供对应安全服务。在此基础上，飞书科技对服务器的访问具有加强的安全控制，所有服务必须通过堡垒机进行操作并进行审计。通过白名单来控制业务服务的访问来源，保证服务只有信任来源可以访问。

飞书科技设置了严格的员工访问控制策略来限制内部资源的访问。员工访问内部资源需要进行身份验证，确认身份后，员工默认仅有最小权限。新的权限获取，需要经过相关负责人员审批并记录。权限具有有效期，在有效期结束后，系统将自动回收权限。员工对线上服务的操作需通过堡垒机进行，所有操作日志均长期保留，以备审计使用。
所有员工在公司网络边界外，都需要通过VPN连接来访问公司内部资源。公司内审与内控部门会对访问日志等进行审计，发现并追溯违规操作记录，并进行相应的处罚。

5.2 DDoS及网络攻击防御

飞书科技服务通过CDN、动态加速来为客户提供网络接入访问，并且通过公司负载均衡访问后端服务；在遇到针对机房的DDoS攻击时，通过网络接入服务商（如中国电信等）提供的清洗服务来进行攻击防御。

5.3 网络传输加密

飞书科技产品在内外网均采用HTTPS、WSS进行传输，保证了传输过程的安全，保证信息不会被中间人篡改、窃取 。

六.服务器安全

飞书科技使用自有机房的物理服务器、云服务器为客户提供服务。飞书科技采取了一系列安全管控措施，保障服务器生产安全，有效防范网络恶意攻击行为。

6.1 服务器访问控制

飞书科技定期对服务器资产进行扫描，及时关闭非必要的端口及服务，保障对外权限最小化，过滤不安全的服务，降低安全隐患。安全人员定期进行弱口令检测，督促服务器运维人员提升密码复杂度，防范暴力破解。

6.2 漏洞扫描

飞书科技采用自动化的漏洞扫描工具定期进行服务器漏洞检测，由安全人员确认后第一

时间通告给相关人员进行处理修复，且运维人员会定期进行系统补丁更新，有效保障服务器稳定运行。

6.3 入侵检测

飞书科技自有机房物理服务器全面部署了HIDS（服务器入侵检测系统），可以实时监控服务器文件基线变更，发现异常进程、捕捉主动异常外连、木马后门等异常行为，并及时作出响应。另外对于来自客户端的所有流量都经过WAF（应用防火墙）进行攻击检测和验证，确保其安全性与合法性，对恶意的请求予以实时阻断。安全团队会密切跟踪安全态势和最新的攻击手法，研究入侵特征，并定期升级防御策略。

6.4 异常检测

构建于大数据平台和机器学习平台之上，安全团队对服务器产生的海量主机日志和自研 HIDS 采集的数据进行多维度的安全分析，建立异常检测模型，及时发现服务器上的风险操作、异常进程、恶意网络连接等异常行为，并及时作出响应。安全团队会密切跟踪安全态势和最新的攻击手法，不断迭代安全算法模型，能够更新异常行为特征，并定期升级防御策略。

七. 应用安全

飞书科技通过安全开发流程保证产品安全。

7.1 安全开发流程

飞书科技力图从安全漏洞的源头控制安全隐患。通过制作安全课程，并以现场及网络课堂的形式提供培训，所有开发人员、产品经理都要接受安全培训，了解相关的安全漏洞成因及编码知识。安全团队在项目启动时，与项目经理进行沟通， 确保安全需求、安全测试在项目计划中体现。同时安全团队会对产品使用的第三方库、工具进行评估以及漏洞挖掘，确保没有供应链引入的漏洞。安全团队会与产品团队一起进行设计和编码的安全性审阅。在产品上线前，会进行渗透测试以及部署的安全评估，来保证服务的安全性。

7.2 用户账号安全

用户对飞书系统的访问，可以通过密码加动态验证码的方式来进行身份的认证。对于未识别的设备发起的登录，风险控制策略会增加其登录验证难度。同时账号系统具有对异常、暴力登录企图的防御能力。

飞书接入自研的风控与反作弊系统。具备反恶意注册、反撞库、反暴力登录破解等防护功能。用户采用密码+动态密码多因素验证登录，可以有效避免因密码丢失导致的账号泄露。

7.3 漏洞与安全事件管理

飞书科技通过多种手段监控内、外部安全漏洞与威胁情报信息。安全团队采用自动化的安全扫描工具对自身服务、操作系统进行扫描，通过定期的渗透测试对应用系统进行安全检查。漏洞及威胁情报信息经安全团队确认后，将根据危害情况，确定风险等级，并第一时间推送至相关部门进行修复处理，公司拥有完善的漏洞生命周期管理策略，专业的安全团队跟进所有安全问题的解决。

同时，飞书科技安全团队与业界顶尖第三方测评公司、白帽社区保持密切的合作与沟通，会不定期邀请外界公司及白帽子对服务进行渗透测试，并给予其奖励，以发现尽可能多的安全漏洞。

飞书科技安全团队执行7*24应急响应策略，安全事件发生时，安全团队会根据安全应急预案迅速对事件做出等级划分，并启动应急响应流程，阻止安全事件扩大。安全事件处理完成后，会对事件进行复盘，复盘内容包括事件发生的原因、事件处理的过程及结果、事件主要负责人及后续跟进措施等内容，并记录复盘结果和后续跟进措施，保障事件闭环。

八.数据安全

飞书科技对数据具有完整的生命周期管理，从数据的创建、存储、传输、使用、销毁都有明确的流程和技术保障，公司拥有相应控制措施以确保数据传输、数据存储、数据访问以及数据销毁流程的安全性。

8.1 数据传输

飞书科技为租户提供了支持强加密协议的数据传输链路，消息拉取、身份验证、操作指令等数据传输均使用HTTPS进行加密并使用2048位RSA密钥；消息推送通过WSS协议对所传输的数据进行加密保护；视频聊天采用端对端加密以保障数据传输的安全；云文档服务采用对称加密算法AES256进行加密后传输。

8.2 数据存储

飞书科技使用安全的密钥机制对数据进行加密存储，我们对所有消息及云文档数据及招聘简历数据都进行了加密存储。

飞书科技制定了完善的数据分类分级管理办法，对飞书办公套件收集的用户信息、后台管理系统中的租户信息等都进行了严格的分类分级管理，并对所有系统中存储的敏感信息进行了加密处理，有效保障用户信息安全。

加密算法内嵌于各应用源代码中；密钥由密钥管理系统（简称“KMS系统”）产生，并由各应用调用。KMS服务负责密钥和敏感配置信息的生命周期管理，包括创建、存储、分发、使用、更新、删除等。飞书用户的数据加密使用的主密钥和飞书服务的各种其他敏感信息（如数据库账户、密码等）均存储于飞书维护的KMS系统中，访问需通过KMS接入进行。KMS系统的主密钥使用密钥共享协议生成多份密钥分 量，分发给不同职能角色进行管理，提供大于总数一半以上的密钥分量才能还原KMS系统的主密钥。KMS主密钥会定期轮转更新，提高KMS数据的安全性。

8.3 数据访问

用户数据的访问，均进行了严格的权限隔离。用户之间在没有授权的情况下，无法互相访问。对数据的访问必须通过数据所有者显式的授权，比如共享操作等来完成。

飞书科技员工对用户数据的访问被严格限制和审计，员工默认没有对任何用户数据的访问权限。特殊的访问需求要经过用户的显式授权以及内部严格的审批流程，才可以获得临时访问权限，在操作完成后权限将立刻被收回。飞书对数据的操作均有详细日志记录，并区分不同操作者角色，授予不同的权限。操作需要进行审批并进行审计。

我们不会公开披露您的信息，除非获得您的同意。但根据法律法规、强制性的行政执法或司法要求，在必须提供您个人信息的情况下，我们可能会依据要求的个人信息类型和披露方式向行政执法或司法机构披露您的个人信息。当我们接到披露请求时，在符合法律法规的前提下，我们要求其必须出具与之相应的法律证明文件，我们仅提供执法部门因特定调查目的且有合法权利获取的数据。在法律法规许可的前提下，我们披露的文件均在加密措施的保护之下。

8.4 数据销毁

在终止对用户服务时，飞书管理员会删除用户账户信息，在符合当地法律法规的前提下，永久删除用户数据。磁盘报废均需经过消磁处理并销毁，确保无剩余信息。

用户机构的离职员工可向租户管理员提出账号注销申请，由用户机构确认离职员工账号内的群主、日程、文档等数据已被转移后，租户管理员通过飞书的客服功能联系公司。公司根据用户机构租户管理员的申请，对需注销的账号相关的数据及文档进行去标识化处理。

公司在与用户机构签订合作协议时，与用户机构约定，当终止合作时，将根据用户机构提出的数据销毁要求销毁对应数据。

除供企业租户内的用户使用外，飞书办公套件亦支持个人用户使用。若个人用户需注销账号，须通过飞书的客服功能联系公司，公司将提供具有账号注销功能的飞书办公套件

安装包。安装该版本后，用户可通过软件提交注销账号申请，飞书办公套件自动根据申请对后台数据库中该账号相关的数据及文档进行去标识化处理。

8.5 数据安全检测

飞书科技的线上环境所有服务器的登录行为、操作行为、服务器安全基线文件变更、访问权限变更和数据访问行为都会被记录。安全团队通过建立用户行为画像和异常行为模型，实现异常行为的识别、分析和关联，自动化实时检测各种异常数据访问行为，如对数据的非法访问、恶意数据爬取和风险操作、登录异常、权限升级等，并进行告警或阻断。

九. 物理基础设施安全

飞书科技采用自有基础设施为全球不同地区的客户提供服务，公司制定了数据中心安全管理制度，明确规定了机房访问管理、机房环境安全等要求，并采取了完善的措施保障基础设施安全。

9.1 物理访问授权

飞书科技使用自有基础设施，包括机房、传输、网络设备、安全设备、服务器等。系统部负责飞书科技基础设施的维护和安全。飞书科技使用的自有机房按照Uptime Institute Tier3以上等级建设，达到了非常高的可用性标准。数据中心由专业人员进行日常维护，并设有7*24监控，访客若需进入数据中心，必须提前通过专用系统进行申请，获得审批同意后，且在入口处需要经过安全检查和登记携带物品才可进入。

9.2 运营管理安全

机房管理人员每月进行数据中心巡检并形成月报，同时公司安全部门至少每年进行一次数据中心巡检，巡检内容包括基础建设环境管理、人员访问和权限管理及资产安全管理等，并出具巡检报告，巡检结果通报至系统部，由系统部就其中发现的异常及时进行处理。

十. 灾难恢复与业务连续性

10.1 备份与灾难恢复

飞书科技制定了相关规定，对办公套件的备份策略、备份数据保管和备份恢复性测试等方面进行规范。业务数据库均有定期快照和备份，数据两地三备份存储，同时公司部署了备份执行情况监控机制，确保数据备份的完整性。飞书科技定期进行备份数据恢复性测试。

10.2 业务连续性保障

业务系统接入层均采用高可用方式接入，通过基础服务提供商提供的公共网关服务接入。后端采用多实例接入，保证服务的可靠性。对流量和故障做细致监控，在流量突发、或者故障时，采用降级运行方式保障业务可用性。

飞书科技针对可能导致业务中断的场景制定了应急响应和恢复措施。每年执行一次业务影响分析和风险评估，识别重要业务流程和可能造成公司业务与资源中断的威胁；定义最大可容忍中断时间、恢复时间目标和最小服务水平等指标；针对不同业务的中断场景制定应对策略。

10.3 应急演练

飞书科技具有完备的应急演练机制，定期进行故障演练，参加人员包括业务团队、安全团队、运维团队等。至少每年对可能导致业务中断的情况进行一次灾备演练以保证数据的可用性。

十一. 变更控制

11.1 程序变更

飞书科技制定了完善的程序变更管理规定，明确了变更管理要求及流程，包括变更方案制定、变更审批及变更实施等。对线上服务的稳定性、可用性、安全性造成已知或潜在

影响的操作，均属于线上变更范围。飞书产品开发严格控制变更操作，防止变更操作影响服务的稳定。线上操作必须有操作单，批准后才可进行。公司为各产品相关应用部署了独立的开发、测试及生产环境，变更操作遵守灰度发布上线，上线均需进行小流量测试，才可正式发布，以此确保服务的稳定和安全。

11.2 源代码控制

飞书科技制定了严格的源代码管理流程，研发人员仅可访问和管理其所属团队对应的代码仓库。代码仓库中各项目代码仓设置了代码仓负责人，研发人员如需申请其团队以外的代码仓库访问权限时，须在代码仓库中提交申请，经其部门主管和所申请的代码仓库负责人审批后，才可添加相应权限。

11.3 基础架构变更

飞书科技在公网边界部署访问控制列表对网络访问进行控制。若需对ACL配置基线及网络访问控制列表进行变更，运维人员通过平台提交申请，由专业工程师对变更合理性进行判断后执行操作。仅授权的工程师拥有执行网络访问配置的变更操作权限。

11.4 变更监控

飞书科技每年执行内部审计以检查公司内部控制体系的运行情况，其中涵盖对变更管理相关控制的执行有效性检查，并将结果汇总在内部审计报告中。若发现异常，由内审部门和相关负责团队沟通并跟进整改结果。变更管理过程中存在不兼容职责的分离，包括变更开发、测试、批准、发布及监控。