企业微信

企业微信安全白皮书

企业微信团队

【版权声明】

【商标声明】

【服务声明】

本白皮书仅供参考。对于本白皮书中所描述的信息和内容，企业微信不作明示、默示的保证。本白皮书基于现状编写，在本白皮书中的信息和意见，包括网址和其他互联网网站参考，均可能会改变，恕不另行通知，您将承担使用它的风险。

本白皮书未授予您任何腾讯产品的任何知识产权的法律权利。

如对本白皮书有任何疑问或投诉、建议时，请通过 https://kf.qq.com 与我们联系，或将您的问题发送至 Dataprivacy@tencent.com。

版本变更记录		
时间	版本	说明
2017 年 6 月 29 日	企业微信白皮书 V1.0	版本创建
2018 年 6 月 21 日	企业微信白皮书 V2.0	内容更新
2018 年 9 月 20 日	企业微信白皮书 V2.1	内容更新
2019 年 8 月 20 日	企业微信白皮书 V2.2	内容更新
2022 年 3 月 1 日	企业微信白皮书 V2.3	内容更新

序言

随着互联网时代的发展，企业办公沟通工具变得更加便捷，应用场景越来越丰富。与此同时，当前的互联网业务也时刻面临着各类风险和挑战，国内外数据安全事件愈加频繁，保障数据安全，防止数据泄漏与滥用，预防黑产攻击和不良信息骚扰等成为了许多企业和 APP 移动应用面临的难题。

企业微信一直致力于让每个企业拥有自己的微信，帮助企业以连接为基础，实现智慧管理、智慧生态、智慧服务，并为企业用户提供全面安全保障。安全一直都是企业微信发展过程中的一项重要基本原则，企业微信联合腾讯专业安全团队，凭借自身实力优势和多年积累的互联网安全技术与红蓝对抗经验，目前已建立强大的网络安全保障体系，以保护用户隐私和企业数据，企业微信作为行业标杆，其网络安全得到行业广泛认同，信息安全管理体系获得了国际权威机构认可。本着“用户为本，科技向善”的价值理念，企业微信持续为国内外百万余家企业和腾讯内部 10 万名员工提供安全、专业、可靠的服务。

本白皮书将与读者分享企业微信安全理念和保护实践，介绍企业微信在合规性、数据安全、运营安全、基础安全等方面所做的努力，以加强企业和用户对企业微信网络安全保障能力的了解。企业微信能从容应对互联网各类攻击，防范用户信息泄露，保护企业和用户信息安全。

1 企业微信安全理念

企业微信，让每个企业拥有自己的微信。

作为一款企业级即时通讯和办公协同平台，企业微信具备与微信一致的沟通体验，支持企业内部的即时沟通、移动办公、音视频会议、一体化集成化办公等多种功能，拥有强大的生态开放能力和丰富的办公应用，满足企业与上下游合作伙伴的沟通协作，触达微信 C 端个人用户，构造完整的用户服务体系，提供各种企业服务能力连接。同时，企业微信将安全支持作为最核心的产品竞争力进行打造，实现高度安全的私有化部署，采取高强度的数据加密技术，提供高度复杂的网络安全支持。

企业微信高度重视网络安全，一直视安全为自己的生命线，始终践行"用户为本，科技向善"的价值理念，坚持一切以用户价值为依归，将社会责任融入产品及服务之中，敬畏规则守护公义，以安全促发展，助力行稳致远。

2 合规性

2.1 合规建设

企业微信以维护国家网络安全与用户个人信息安全为己任，严格遵守《中华人民共和国网络安全法》及相关法律、法规和规范性文件，切实履行企业网络安全主体责任。企业微信基于合规和业务安全要求，以信息安全管理体系国际标准和国家网络安全等级保护国家标准为蓝本，遵循风险管理的理念，建立健全内部安全合规管理体系，积极通过国家权威机构测评认证和国际安全资质认证以及行业合规认证，率先完成信息安全国际标准认证“大满贯”，切实保障企业微信产品与服务持续的合规性、安全性和可靠性。

2.2 资质认证

目前企业微信已经获得的权威合规认证包括：国家网络安全等级保护测评（第三级）、ISO/IEC 27001、ISO/IEC 27018、ISO/IEC 20000、SOC2 Type1、SOC2 Type2 服务组织审计报告。

国家网络安全等级保护测评（第三级）是中国权威的网络安全等级资格认证，是国家对非银行机构的最高级认证，属于“监管级别”。网络安全等级保护制度是国家网络安全保障的一项基本制度，是保护信息化发展，维护国家网络空间安全的根本保障。企业微信通过国

家网络安全等级保护第三级备案和测评，表明企业微信整体上具备较高的网络安全防护水平，其信息数据安全管控能力获得国家权威部门认可。

ISO/IEC 27001:2013 信息安全管理体系标准是国际上针对信息安全领域最权威、严格，也是最被广泛接受和应用的体系认证标准。企业微信通过国际知名的第三方认证机构审核并获得认证，表明企业微信的安全管理体系已达到国际先进水平，可为企业和用户提供更安全、更可靠的服务。

ISO/IEC 27018:2019 公有云个人信息保护管理体系标准是国际标准化协会制定的一项国际标准，是公有云个人隐私数据保护方面的首个国际标准，得到了全球广泛认可。企业微信通过国际知名的第三方认证机构审核并获得认证，成为国内首家获得此项证书的企业办公产品。

ISO/IEC 20000-1:2018 信息技术服务管理体系标准是国际标准化协会基于 IT 服务管理最佳实践提出的一套 IT 服务管理体系标准，该体系旨在帮助 IT 组织识别并管理 IT 服务的关键流程，保证向业务和客户有效地提供高质量的 IT 服务，已成为组织的 IT 运营和服务交付管理水平的国际标准，得到了国际社会的普遍认可和采纳。企业微信通过国际知名的第三方认证机构审核并获得认证，表明企业微信能够为客户提供高质量的 IT 服务，以满足企业和用户的需求。

SOC 审计报告 （系统和机构控制报告，System and Organization Controls Reports）是由国际专业的第三方会计师事务所依据美国注册会计师协会（AICPA）相关准则出具的服务机构的系统和内部控制情况相关的审计鉴证报告。 自 2018 年企业微信获得 SOC2 Type1 审计报告起，2019 年至 2021 年，企业微信连续三年获得由全球知名的第三方会计师事务所出具的 SOC2 Type2 审计报告，是中国大陆首家获得基于安全性、保密性和隐私性原则的 SOC2 Type2 审计报告的企业办公产品，企业微信持续通过 SOC2 Type2 的严格审计，证明企业微信对个人隐私保护和数据安全执行了最严格标准，有力保障企业与用户数据安全。

2.3 个人信息保护

腾讯视用户个人信息安全和隐私保护为“生命线”，仅在法律规定及协议约定的范围内合规使用用户数据。企业微信致力于保护用户个人信息，并严格遵守中国以及经营所在地国家或地区的法律法规，企业微信的隐私政策向社会公众开放，可以在官方网站上获取（《企业微信隐私保护指引》官方网站：https://work.weixin.qq.com/nl/privacy），如有投诉、建议、未成年人个人信息相关问题，可通过 http://kf.qq.com 与腾讯客服联系，也可以将问题发送至 Dataprivacy@tencent.com 或寄到中国广东省深圳市南山区科技中一路腾讯大厦 法务部

数据及隐私保护中心（收）。

企业微信秉承腾讯“科技向善，数据有度”的隐私保护理念，遵循腾讯隐私保护方法论 P·B·D（Person·Button·Data），致力于实现安全、自主、合规、透明的隐私保护目标，并根据自身业务特性理解并进行实践，实现全方位的个人信息保护，为企业和用户提供持续稳定和安全可靠的服务。

企业微信在信息安全和隐私保护实践上遵守 ISO/IEC 27001 和 ISO/IEC 27018 国际标准和 GB/T 22239 网络安全等级保护第三级安全要求。

3 数据安全

近年来，个人信息保护和数据安全成为社会公众关注的热点话题，随着《中华人民共和国网络安全法》、《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等法律法规及国家标准相继出台，社会各界对互联网公司个人信息处理活动高度关注。腾讯秉承“科技向善，数据有度”的价值理念，视用户个人信息安全与隐私保护为自己的生命线。企业微信重视数据安全，建立了安全可靠的数据安全保障机制和安全技术体系，为客户数据的全生命周期，包括数据收集、传输、存储、使用、共享、销毁等各个环节提供强有力的保护，确保合法合规，全方位保护客户的数据安全。

3.1 数据收集

企业微信收集数据遵循合法、正当、必要的三大基本原则，仅最小化收集实现产品功能所必要的信息。在收集敏感信息时，主动提示数据被采用的目的和用途，并按数据的敏感程度进行分类，后续数据的处理过程严格按照数据类别要求进行管控和处理。

3.2 数据传输

数据传输安全是对数据进行网络传输的安全管理，这是数据安全防护的重要阶段，也极易发生数据安全事件，如数据泄露、窃取、篡改等安全事件。企业微信终端和服务端的网络通讯使用 TLS 协议，同时应用层也对传输数据进行加密和校验，保证数据传输安全。

3.3 数据存储

企业微信在数据存储方面实行了严格的安全管控措施，包括但不限于访问控制、身份鉴别、安全配置、防泄漏、加密、脱敏等措施。企业微信按照数据分类，对企业、用户重要类别数据包括组织架构、文本消息、文件、图片等数据进行加密存储。不同企业使用不同的密钥进行加密，保证数据的机密性和安全性。密钥由统一的密钥管理系统进行管理，保证密钥的传输安全，大大提高加密的安全性。不同类别的数据存储在不同的物理磁盘或者机房，从物理上隔离不同类别数据的存储环境，提高重要类别数据的安全性。

与此同时，企业微信严格遵守国家法律法规的规定，会明确告知用户数据存储的目的、方式、安全措施及安全风险等。

3.4 数据使用

企业微信确保不超出《企业微信隐私保护指引》及与客户签订协议中所指定的使用目的，同时确保采取个人信息访问控制措施，按照最小授权原则，使申请方仅能访问职责所需的最小够用的个人信息，仅具备完成职责或产品功能所需的最小数据操作权限，且授权确保有时限，到期回收权限，如需再用，须重新申请和审批。

终端用户身份验证通过后，系统会下发用户票据，数据的访问和使用通过票据管理系统严格管控访问权限，防止越权、非法访问。同时服务端系统模块也接入票据管理系统，对模块级别票据也有严格管控，防止内部越权、非法访问。

3.5 数据共享

企业微信在数据共享交换方面，进行了严格的控制，明确了数据共享交换各环节需要采取的安全措施。目前，企业微信除《企业微信隐私保护指引》及与客户签订协议中定义的数据共享、转让和披露场景外，不会主动与第三方共享、转让或披露用户的个人信息，如存在共享或转让用户的个人信息，或用户授权或请求将与其相关的个人信息披露给特定的第三方的情形时，企业微信会直接或确认第三方征得用户对上述行为的明示同意。此外，企业微信还会对该行为进行安全评估。企业微信对第三方有严格的要求和审计机制，上架应用必须符合相关的要求和通过严格的安全测试。第三方应用如果使用用户或企业数据，必需经过授权。

企业微信确保不将在中华人民共和国境内运营中收集和产生的个人信息传输至境外。当由于业务需要向境外提供个人信息时，企业微信确保按照有关部门制定的办法和相关标准进

行安全评估，并符合其要求。

3.6 数据销毁

为充分保证数据销毁后的不可逆性，企业微信根据国家相关要求，结合腾讯安全管理制度和严格的逻辑删除和物理擦除方式，对退役报废、带离数据中心的存储介质或带有存储介质的设备进行数据删除、硬件消磁及物理销毁处理，确保销毁过程安全可靠，经过销毁后的数据无法被非法恢复。

3.7 数据安全审计

通过恶意设备检测、票据越权限检测，企业微信对异常行为进行发现和告警，对异常登录，非法访问数据可以有迹可查。

4 终端安全

企业微信提供终端设备类型识别、登录保护、恶意设备识别等终端安全保护能力。通过使用加壳、混淆、签名校验等手段防止程序被反编译、篡改。具备模拟器、恶意设备指纹等检测能力。

在终端数据加密的场景，支持密钥内存存储，避免密钥本地存储风险，大大提高加密过程的安全性。

5 访问控制安全

企业微信对业务使用提供基于角色的访问控制、账号保护、多因子身份验证、单点登录等安全能力。访问管控使用票据技术控制用户访问权限，严防越权、非法访问。同时服务端系统模块也接入票据管理系统，对模块级别票据也有严格管控，防止内部越权、非法访问。

密钥由统一的密钥管理系统进行管理，保证密钥传输安全性和保密性。

6 运营安全

6.1 组织与人员安全

为贯彻落实企业微信的安全理念，企业微信从组织层面整体考虑和设计，制定了一套完善的网络安全管理制度，并持续不断地加强安全资源投入，配置专业安全管理人员。

企业微信深知，在做好业务全生命周期各环节安全的同时，不能忽略员工的安全行为规范。企业微信的员工入职前通过合法的背景调查，以确保员工符合公司行为准则、商业道德、信息安全要求。

入职后，所有员工需要签署公司保密协议，从法律和制度层面约束员工的操作行为。腾讯向来注重客户信息和用户数据保护，泄露客户信息及用户数据行为属于公司高压线之一，在入职培训中重点强调。

企业微信运营管理团队的人员变更均由统一运营管理门户实现自动化权限控制：入职时自动赋予基本的默认权限，调职时自动修改岗位权限，离职时自动禁用所有权限。员工可在统一运营门户中申请所需的临时或固定权限，在获得多级评审和批准后，系统将自动赋予其新的权限。临时权限在使用期限结束后自动回收。

企业微信会定期对员工进行安全培训，包括安全意识、安全技术、安全红线等，确保员工的安全意识和职业操守。

6.2 持续对抗黑产

企业微信安全团队基于微信亿级用户的安全防护经验， 7*24 小时进行安全监控，持续对抗黑产。定期进行攻防演练，主动聘请第三方安全公司进行安全评估和测试，经受专业安全考验。同时联合腾讯各个安全领域专家，进行专项讨论和研究，对可能存在的安全漏洞进行扫描和测试，实施主动防范。

腾讯专业的安全团队包括：科恩、玄武和云鼎等实验室，汇聚了国内安全领域顶尖的“白帽”安全专家和研究人员，为企业微信安全提供了坚实的后盾。

6.3 应急响应

企业微信定制了完善的应急响应流程、人员的详细职责和联系方式，并严格按照要求进

行定期演练，确保容灾恢复预案的及时性与可行性。

企业微信安全响应中心平台还联合腾讯安全应急响应中心制定了突发安全事件的处置流程和标准，处置流程包括：预报告阶段、报告阶段、处理阶段、修复阶段、完成阶段。企业微信将尽最大可能保障用户信息安全、数据安全。

7 基础安全

7.1 物理和基础架构安全

作为企业级即时通讯和办公服务提供商，企业微信着力为每一个客户提供安全、稳定、持续、可靠的物理设施基础。企业微信依据数据中心相关的国际标准和监管要求，联合腾讯云建立了一套全方位的安全管理体系，从制度策略，到流程管理，并配合严格的访问控制和监察审计，通过持续改进来保证数据中心的物理和环境安全。

7.2 主机与网络安全

7.2.1 网络通信安全

终端和 web 管理端与企业微信后台的通信都受到了 TLS 安全协议的加密保护。

此外，企业微信的 API 所提供的所有接口具有 TLS 加密、签名校验、状态监测等安全能力，能为企业通信安全保障。

7.2.2 DDoS 攻击防护

企业微信为您提供高效的分布式防护能力。其中，BGP 高防，接入 21 线 BGP 线路，全面覆盖国内外主流运营商，带来极速、稳定的访问体验，同时拥有 4T 防护带宽，是国内最大的 BGP 高防产品。

7.2.3 网络接入安全

企业微信所有外网接口统一由负载均衡（Cloud Load Balancer，CLB）进行处理，CLB 具有高性能、高可用、安全稳定等特点，可提供安全快捷的流量分发服务，访问流量经由 CLB

可以自动分配到云中的多台云服务器上，扩展系统的服务能力并消除单点故障。支持亿级连接和千万级并发，可轻松应对大流量访问，满足业务需求，并且 CLB 依靠大禹分布式防御系统能够防御绝大多数网络攻击（例如 DDoS、CC、Web 入侵），保护更加高效和安全的网络访问。

7.2.4 网络隔离

企业微信制定了严格的内部网络隔离规则，通过物理和逻辑隔离方式实现内部的办公网络、开发网络、测试网络、生产网络等的访问控制和边界防护；企业微信确保非授权人员禁止访问任何内部网络资源；以及，所有员工如需从公司网络前往生产网络开展日常运维时，都必须经过堡垒机登录生产系统。

7.2.5 网络冗余

腾讯网络出口分多个地域对接多个运营商，构建企业微信网络跨地域的灾备能力，有效地降低运营商公网故障带来的持续性影响。

基础网络采用 N*N 的冗余建设方式，配合路由层级的路径优先和路由可达性的流量工程调度，确保网络服务不会因为单点设备故障而中断。计算节点也是采用 N*N 的冗余建设方式，单一计算节点在故障发生时通过调度器实时自动剔除，有效保障用户业务的可用性。

8 结语

安全是企业微信的核心，我们始终践行“用户为本，科技向善”的价值理念，持续优化产品与服务的网络安全和个人信息保护实践，以领先的技术和网络安全建设赋能业务安全与合规，提升服务品质，依法保障企业和用户数据安全。

希望以此白皮书分享企业微信在网络安全方面的实践，为办公协同应用发展提供一些方向和思路，与社会各界携手共建良好的网络安全保护秩序。

未来，我们将继续努力，通过完善的安全保障机制和安全技术体系，为用户、企业客户、合作伙伴等提供安全、可靠、有保障的服务，全方位保护用户和企业的数据安全。