企业微信安全白皮书

企业微信团队 | 安全管理部团队

版本变更记录		
时间	版本	说明
2017 年 6 月 29 日	企业微信 1.0	版本创建
2018 年 6 月 21 日	企业微信 2.0	版本修订
2018 年 9 月 20 日	企业微信 2.1	版本修订

目录

1 序言

随着互联网时代的发展，企业办公沟通工具变得便捷，应用场景越来越多。然而，当前的互联网业务时刻面临着各类风险，如：黑产攻击、敏感信息被窃取与滥用、不良信息骚扰等。企业微信借鉴腾讯旗下微信、QQ 等产品多年积累的安全防护能力和经验，目前已建立强大的信息安全体系。企业微信于 2016 年面市后，信息安全体系得到广泛认可，目前正服务于腾讯 4 万多名员工，上百万家企业。

本文将从合规性、数据安全、运营安全、基础安全等方面阐述企业微信信息安全能力，以加强用户对企业微信安全能力的了解。企业微信能沉着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。

1.1 术语

PII：personally identifiable information 个人可识别信息

TGW：Tencent Gateway，腾讯网关

BGP：Border Gateway Protocol，边界网关协议

SaaS：Software as a Service，软件即服务

2 合规性

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，积极获取国家网络安全等级保护认证和国际安全资质认证以及行业合规认证，建立健全内部安全合规体系，率先完成信息安全国际标准认证“大满贯”，有力保障企业微信产品与服务合规、安全、可靠。目前企业微信已经获得的认证包括：国家网络安全等级保护三级认证、ISO/IEC 27001、ISO/IEC 27018、ISO/IEC 20000、SOC2 类型一服务组织审计报告

2.1 资质认证

国家网络安全等级保护三级认证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。企业微信获得了国家网络安全等级保护三级认证，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公安部认可。

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，也是最被广泛接受及应用的体系认证标准。企业微信通过权威审核取得该认证，表明企业微信的安全管理体系已达到国际标准，可为企业和用户提供更安全、更可靠的服务。

ISO/IEC 27018:2014 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。企业微信通过权威审核取得认证，成为国内首家获得此项证书的企业办公产品。

ISO/IEC 20000-1:2011 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，已成为组织的 IT 运营和服务交付管理水平的国际标准，ISO20000 得到了国际社会的普遍认可和采纳。企业微信通过权威审核取得认证，表明企业微信能够提供有效的 IT 服务，以满足企业和用户的需求。

SOC 报告 （System and Organization Controls Reports 系统和机构控制报告）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）的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。企业微信通过了 SOC2 的安全性、保密性和隐私性原则的审计，是《中华人民共和国网络安全法》及国家标准《个人信息安全规范》正式实施以来，国内首个获得隐私性原则审计 SOC2 Type1 报告的企业办公产品，同时也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。

2.2 安全合规性

企业微信未使用第三方服务商处理用户的 PII 数据，用户委托第三方向企业微信提交 PII 数据时，需要确保第三方遵守相关保密规定。

未经用户同意，企业微信不会向第三方披露用户的 PII 信息，除非法律另有规定。

企业微信对外提供的服务为 SaaS 服务。

用户 PII 数据存储于中华人民共和国大陆地区。

若发生 PII 数据泄露等安全事件，我们会启动应急预案，阻止安全事件扩大，并最迟不迟于 30 个自然日内将事件相关情况以邮件、信函、电话、推送通知等方式告知你，如果难以逐一告知时，我们将采取合理、有效的方式发布公告。

企业微信在安全实践上遵守 ISO27001 和 ISO27018 国际标准。

3 数据安全

近年来，个人信息相关法律法规相继出台，政府、媒体等社会各界对互联网公司个人信息处理活动高度关注。企业微信对个人信息处理包括：数据产生、传输、使用、存储、销毁等各个关键环节都有安全保障措施，都确保合法合规。

3.1 数据产生

用户使用企业微信过程产生的数据，会根据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

终端和服务端的网络通讯使用 SSL/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 数据使用

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。

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。

3.4 数据存储

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。

3.5 数据销毁

企业微信根据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。

3.6 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 人员安全

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，员工必须签署保密协议。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。

企业微信会不定期对员工进行信息安全培训，确保员工按即定的安全策略执行。

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、湛泸、反病毒、反诈骗、移动安全和云鼎等实验室，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

作为企业通讯服务提供商，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，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。

7.1.1 基础设施安全

电力、空调、消防和静电防护等基础设施安全对企业微信数据中心机房来说是最为基础的要求，也是保证可用性最重要的方面之一。

企业微信各数据中心均按照相关国际标准和当地安全要求进行选址、建设或租赁。各数据中心电力系统和空调系统均采用高稳定性全冗余系统，在任意单设备故障情况下，均能确保数据中心的电力和供冷持续性；各数据中心均配备完整的消防系统，包括定点区域火灾侦测系统、自动气体灭火系统以及供紧急使用的手动灭火装置；各数据中心内部全部安装防静电地板，机柜、线槽等，且均安装接地线，用以防御静电给设备带来的损害。此外，企业微信还要求所有机房管理人员定期接受业务连续性应急演练培训，以确保数据中心基础设施的安全保障得到有效落实。

7.1.2 访问控制制度

企业微信根据设备的重要性对数据中心不同区域定义了的三类安全级别：包括一般安全区域、受限安全区和高度受限安全区。

各数据中心根据不同级别的区域安全要求制订了严格的基础设施和环境访问控制。根据数据中心人员类别和访问权限，建立了完整的人员访问控制安全矩阵，实现对数据中心的各类人员的访问、操作等行为的有效管控。其中，门禁授权系统按照不同安全等级和不同功能的区域进行划分，各类来访或工作人员出入数据中心均需进行身份核对和随身物品检查，并登记携带物品。从环境控制角度，各数据中心对车辆进出也有严格的管理规定和控制措施，所有员工个人车辆、供应商货车等都需进行车辆信息登记，且仅允许获得授权的车辆进入数据中心周边环境。

7.1.3 安全检查和审计

企业微信各数据中心的安保人员每日均严格根据巡检清单和巡检计划对各机房和设备情况进行巡检，巡检频率不低于每 2 小时/次，并在每个检查点签名并记录检查时间，一旦发现安全违规事件，会立即启动数据中心机房管理紧急流程。

各数据中心均已制订了物理安全应急预案，并定期组织数据中心工作人员进行安全演练。一旦发生物理安全事件，该预案将能够立即生效并指导相关人员以最大可能保护客户资产。

同时，为了确保上述措施和规范的落地执行，企业微信统一建立了定期安全审计管理制度，每个季度对物理安全现场操作和管理进行审计，并输出内部审计报告，跟进和推动物理安全审计风险点的改进。

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 SSL/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 SSL/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 TGW 进行处理，TGW 具有可靠性高、扩展性强、性能高、抗攻击能力强等特点，提供了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，我们始终践行腾讯公司“一切以用户价值为依归”的经营理念，持续加强各项安全控制措施，加强信息安全建设。联合腾讯专业安全团队，致力于互联网安全技术与攻防体系的研究及应用，以保障用户安全。