# 企微云安全白皮书 V5.0

（附：道一信息 ISO27001 信息安全认证；

企微云信息保密承诺书）

企微云致力于为用户提供安全可靠的移动办公服务。信息安全是用户放心使用的基础，因此，企微云一直把安全作为最高优先级目标。我们的信息安全与腾讯的企业微信保持高度一致，并通过多种方式、从多个层面保障企业的数据安全。

企微云通过专门的信息安全委员会来加强信息安全体系建设，并对企微云业务以及整体环境安全负责。信息安全委员会由 CTO，各业务线的安全负责人以及外部专家团队构成，通过高效协作来加强安全管理，应对各种安全威胁，并定期由具备资质的第三方专业机构做安全审计。

## 一、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。依据数据的安全生命周期，企微云对数据创建、存储、使用、共享、归档的整个过程都有相应的保护措施。

### 数据分级

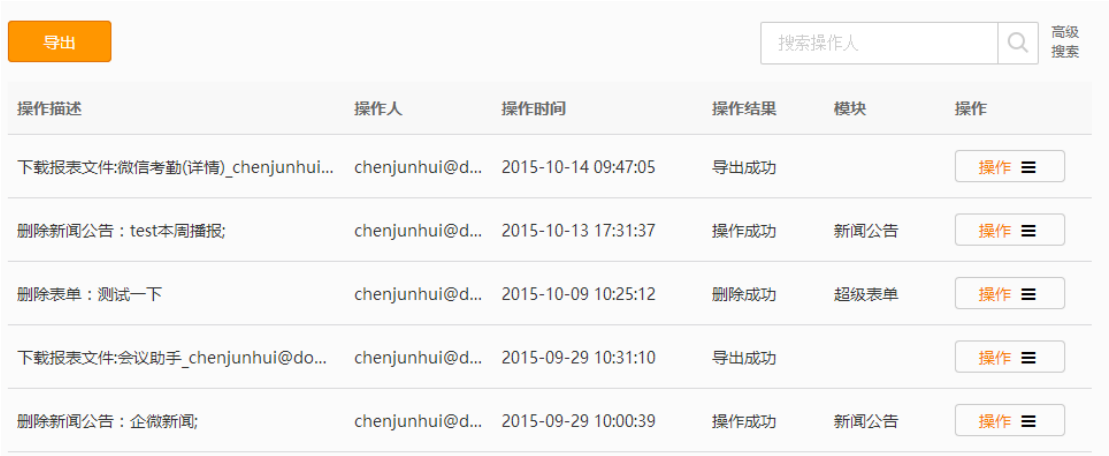
企微对所有用户和企业数据提供存储安全保护。根据存储与使用的数据，实施数据等级保护策略，并按照数据价值和敏感度对数据进行等级划分。根据数据安全的分级，又对应相应的保护策略和要求，以保护用户和企业数据的安全存储。

## 数据使用与防篡改

企微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的控制，以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虫安全保护，以阻断爬虫对敏感信息的爬取。

## 完整的操作日志记录

每一条数据导出、增删均有完整的操作日志可以查询，操作人、操作时间、操作结果一并记录在案。如有异常操作记录，能够及时发现并处理相关责任人。




图一 企微云操作日志

# 二、通信安全

除了数据安全外，信息的传输安全同样重要。企微云采用了多种方式，从传输加密、传输保证、账户认证等多个维度来确保数据的传输安全。

## 网络隔离

企微云通过不同的安全域或物理隔离的网络来实现不同级别的网络隔离。所有的用户接入请求均通过严格配置的 NAT 策略实现，所有的维护请求均通过独

立网络经由 DMZ 完成。对网络的出口处通过端口镜像的方式来甄别各种网络威胁。而内部网络根据不同的用途实现物理隔离，如公共网络，存储网络，心跳网络以及管理网络。

生产网络与办公网络完全隔离，并通过严格的审核机制以及上线流程来保证受信程序或端口的安全访问 ;同时安全专员会定期执行网络安全扫描测试以主动发现可能存在的网络隐患。已实现全站 https 的访问以防止各种网络窃听行为和流量劫持的发生。

## 传输加密

企微采取了一系列的完善措施防止通讯被监听、劫持和篡改，确保了通讯的安全。企微对各项应用通讯进行了全程 SSL 加密，以保证数据安全性。除此之外，企微还针对每个企业设置了唯一的 token 来对通讯内容进行 AES 加密。

## 端到端传输保证

利用对称密码技术对 IP 数据报进行加密 / 解密处理，使得网络中传输的 IP 数据报只有通信双方能够识别 ,可以为互联网络上两台主机之间提供加密的安全通信。安全管理工作由独立的安全服务器完成，采用公钥密码技术向安全客户端传输安全通信所使用的对称密钥，保证端到端的传输数据传输安全。

## DDOS 网络攻击防备

企微云与第三方专业防 DDoS 机构合作，对所有的入站流量实现准实时分析，对异常流量实现及时的手工阻断；与第三方的安全机构合作对关键业务服务器通过监控代理实时上报安全相关的各种数据。当攻击发生时，通过自动化的运维机制，被攻击节点将自动停止服务，并通过第三方专业防 DDoS 机构执行流量清洗后回源到企微云的备用节点，保障服务持续运行。

## 双重认证

企微云支持双重认证，用户除使用普通的密码认证外，也可以使用企业微信的动态身份认证。当用户名和密码丢失后，用户账户和数据仍然可以得到可靠保护，避免被其他人访问。


图二-企微云两种登录方式

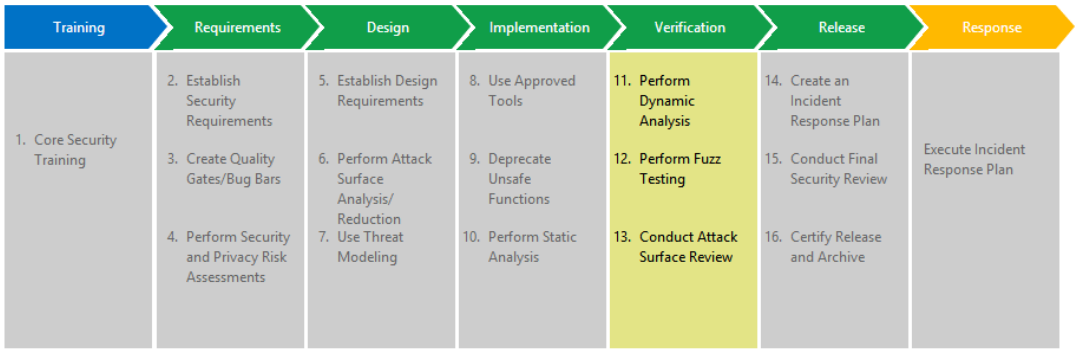
# 三、系统安全

企微云自系统搭建时就完整考虑了系统级的安全方案，从通讯录的权限

到各个应用、文档的访问都有相应的访问控制措施，在确保了外部条件的安全后进一步强化了内部安全。

## SDL 开发流程

企微云在项目开发流程中引入了 SDL（软件安全开发周期）， 借鉴了微软推广 SDL 的经验，并结合企业级安全需求以及企微自身的项目开发流程，从培训、需求分析、开发、测试、发布、运营应急整个过程，控制项目的安全风险。




## 通讯录安全

企微云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的可见性权限； 同时企业可以通过设置来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，方便企业将上下流整合到企微云当中。

对于不同公司的信息，存储空间是相互隔离的。当员工离职并进行离职处理后，将自动剥离员工在该企业的访问权限使其无法访问企业微信中的内容。企微还在企业微信的基础上设置了离职人员复职功能，对于离职人员数据不马上清除，

为工作交接提供了缓冲空间。

企业还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，但不影响其他应用功能的使用。

## 管理权限分级访问安全

企微云各个应用均有独立的访问控制鉴权功能，可以针对每一个应用、每一条数据、表单设置对应的可见范围，访问控制的精度能细化到个人或部门，其他人在非授权情况下无法访问目标数据。保存到企微云的新闻公告、知识百科具有企业访问权限控制，即使被转发给非本企业的用户，对方也无法查看。

## 管理员登录安全

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。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，阻止登录尝试。企微管理员账号还支持与通讯录用户进行绑定，绑定后登录管理后台时会收到登录提醒，如发现收到提醒却不是本人登录，管理员应及时上线修改密码。


图三 管理员登录提醒

## 人员及流程管理制度

**严格的数据访问制度：**在企微，只有技术总监（公司合伙人）具有数据服务器管理权限，并且对数据服务器的维护必须由技术总监亲自操作，不得委托他人。

**规范的客户服务流程：**只有当客户提出需求、认可并授权时，我们的服务人员才会在客户监控下访问客户数据。一切未经客户授权的数据访问，都是被禁止的。

**保密协议的商务保障:** 在客户同我们签署合同的同时还会签署保密协议，确保我公司和个人不会以任何形式泄露客户数据和隐私。

## 数据生命周期管理

企微云对于企业使用过程中所产生的数据以及存储实现全生命周期的管理。其中内部数据存储通过专用的存储网络进行传输，并对产品产生的企业关键数据实现加密存储。存储访问方面遵从严格的访问控制策略，并留存访问痕迹进行审计。

当由于磁盘故障或生命周期结束等原因需要进行更换时，原有磁盘将严格按照相应的标准执行数据清除以及可能的物理销毁。

## 四、物理安全

企微云数据中心包含以下标准的物理安全控制要求：

### 高可用的分布式服务器集群

企微云所在数据中心配备有数十台高性能服务器组成的高性能集群，能确保所有服务的高性能运转。集群内部配有多台备用服务器节点。一旦发现故障节点，可自动接管；因此无论任何节点出现故障，都不会影响整体系统的服务。同时我们还将通过最大限度减少计划内和计划外的停机时间、不间断业务的热升级，来确保各项服务的高可用性。

- 电信级机房比企业的普通服务器机房具备更高的可用性和抗灾。
- 机房安全制度：IDC 机房对进出人员进行严格管理，配备了门禁系统，严格验证进入人员身份，保证机房空间安全性。
- 机房安保措施：数据中心配备专业的保安员 7*24 小时在岗，随时巡视。机房进行 24 小时安全监控，机房内部的所有活动均有摄像记录。

目前部署在跨省市的多个数据中心，通过完备的监控系统实行 7*24 的全方位无死角的系统监控以确保企业的随时随地的业务访问。所有设备及设施所处的机房部署了严格的访问控制和白名单机制，严格审核人员出入来防范可能出现的破坏物理设备等事件。

## 高度冗余的硬件配备

数据中心部署的所有硬件，从防火墙、路由器、交换机，到服务器内部的网卡、电源、硬盘，核心业务及数据服务均实现冗余或主备部署，并部署在多个机房 ,通过多家运营商实现多链路接入 ;数据备份以准实时的方式同步到异地机房，确保在突发情况下，为企微云的持续服务提供保障。；任何一份损坏，都会自动进行切换，并可热插拔、实现在线更换。数据中心采用先进的南北智能双线互联互通方案，同时配备网通及电信专用光纤接入，中国南北及海外用户均可高速访问。

## 健全的灾难防护措施

为保障客户 7*24*365 不间断运作 ,数据中心采用了全方位的防护措施 ,能确保企微云提供的服务不会因为电力故障、火灾、潮湿、高温等气候变化而受到干扰。

关于数据的恢复演练及容灾备份策略，我们针对 DDoS 防御执行每季度演练；针对 MongoDB 利用自己的主从复制技术，采取生成多个副本（本地准实时+异地延时），实现容灾；针对文件类型的数据，利用其自身的复制技术，采取生成多个副本，并定期转储至异地机房，实现容灾。针对其余相关的涉及可用性的演练（如数据库主从切换、机房链路切换、防火墙主从切换等）不定期执行。

## 全天候的自动备份集群

系统所在数据中心配备了强大的备份服务器集群 ,每天凌晨系统将数据备份到灾备中心，能实现强大的全天候自动备份，提供无中断备份和恢复过程，实现全面的数据安全保护。

# 附件一：ISO27001 信息安全管理体系认证证书

道一信息具备 ISO27001 信息安全标准认证，并且在之后的每年都会接收一次安全审查，来确保各项安全策略都实施到位。ISO27001 是信息安全领域的管理体系标准。当企业通过了 ISO27001 的认证，就表示企业的信息安全管理已建立了一套科学有效的管理体系作为保障。

中安认证
ISO27001

# 信息安全管理体系认证证书

经北京中安质环认证中心审核，确认

**广东道一信息技术股份有限公司**

**组织机构代码：75942168-7**

（注册地址：广东省广州市海珠区广州大道南 228 号经典居 29 楼　邮编：510000）

信息安全管理体系符合：

**ISO/IEC27001:2013**

认证范围覆盖如下：

**计算机软件开发和系统集成的信息安全管理活动**

**地址：广东省广州市海珠区广州大道南 228 号经典居 29 楼。**

**适用性声明（SoA）版本号：1.0 版**

注册号：15X10023ROM

有效期:2015 年 09 月 11 日至 2018 年 09 月 10 日

北京中安质环认证中心
(原 8·1 质量体系认证中心)
（地址：北京市朝阳区东三环南路 58 号富顿中心 1 号楼 22 层　邮编：100022）

中心主任：

注：本证书发证一年后与年检标识一同使用有效

| 1监 | 2监 |
|---|---|

证书信息查询方式：
中心网址：http://www.zazh.com
国家认证认可监督管理委员会官网：www.cnca.gov.cn

# 附件二：企微云信息保密承诺书

甲方：企微云接入企业

乙方：企微云

**1.保密内容和范围**

（1）涉及甲方在使用系统过程中产生的业务数据信息，包括甲方保存在乙方服务器上的数据；

（2）凡以直接、间接、口头或书面等形式提供涉及保密内容的行为均属泄密。

**2.企微保密承诺**

（1） 本协议的前提为甲方已对其公司保密信息采取了合理的保密措施，因甲方原因导致的泄密乙方不承担任何赔偿责任；

（2） 乙方应自觉维护甲方的利益，严格遵守本保密规定；

（3） 乙方不得利用所掌握的商业秘密牟取私利；

（4） 乙方了解并承认，通过系统甲方会将具有商业机密的资料（保密信息）保存于服务器上，并且由于技术服务等原因，乙方有可能在某些情况下访问这台服务器。乙方同意并承诺保障甲方数据的安全，如果乙方在未经甲方许可的情况下将数据披露给其他人并经证实而对甲方造成的直接经济损失，甲方有权通过法律途径向乙方索赔；

（5） 乙方同意并承诺，对甲方存储在乙方的关键数据（组织架构、数据、账户密码）进行加密处理，对所有保密信息予以严格保密，在未得到甲方事先许可的情况下不披露给任何其他人士或机构；

（6） 乙方同意并承诺 ,为甲方提供的服务器配备完善的安全设备及防范措施，以保证服务器的安全、稳定运行；

（7） 乙方同意并承诺，保障甲方用以储存具有商业价值资料（保密信息）的服务器所在机房的环境安全；

（8） 乙方同意并承诺，未经甲方同意，乙方不可拷贝服务器上的任何保密信息。

**3.本承诺书中保密义务不适用于以下信息：**

（1）非由于乙方原因已经为公众所知悉的；

（2）由于乙方以外其他不受保密义务限制的渠道被他人获知的信息；

（3）由于法律的适用、法院或其他国家有权机关的要求而披露的信息；

（4）乙方事先征得甲方书面同意而发布的信息。

**广东道一信息技术股份有限公司**

**企微云**