企微大讲堂第十二期回放

企微信息安全与密码管理

（完整版）

- 主讲嘉宾/企微信息安全高级顾问　许亚成

Part One：企微信息安全和密码管理

1、企微如何保护企业信息安全

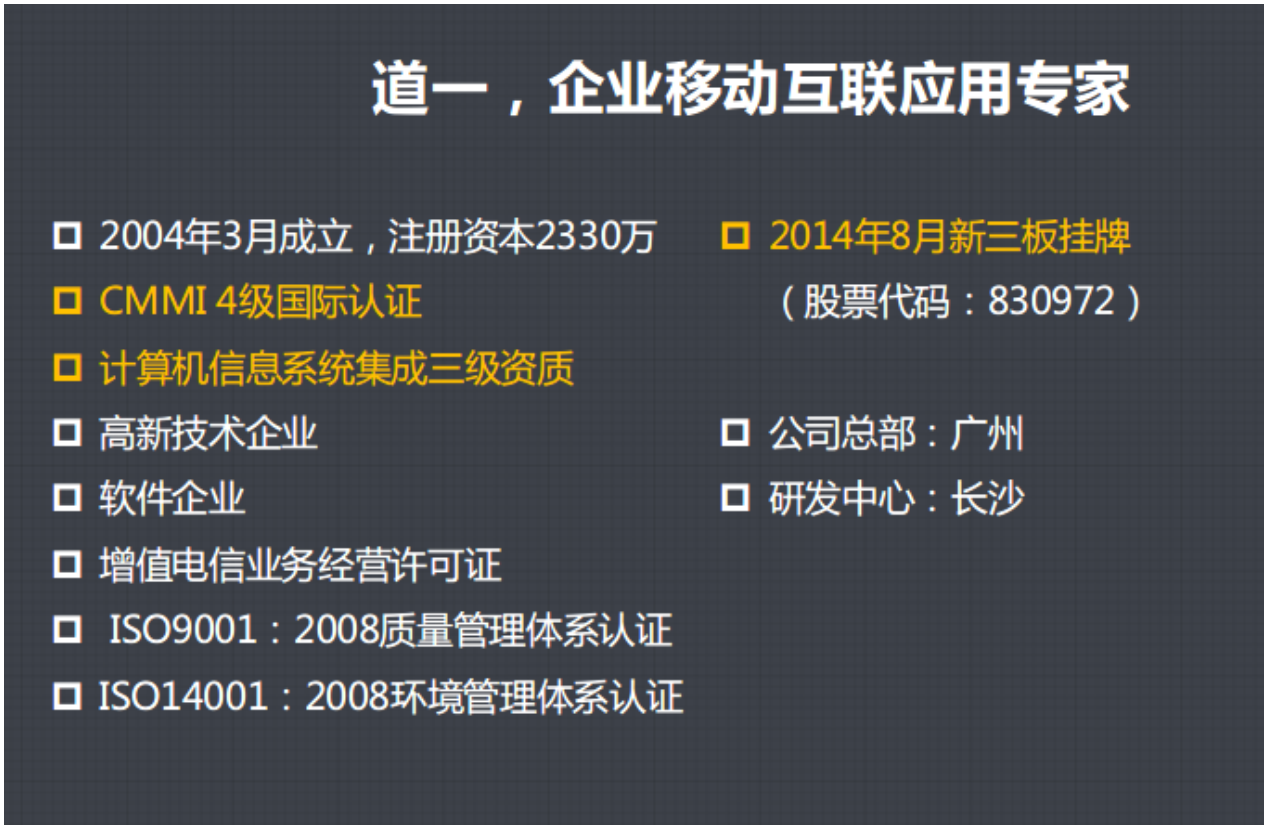
1.1、企微公司的实力

企微云平台是道一信息于 2014 年推出的微信办公平台，道一信息成立于 2004 年，在 2014 年挂牌新三板上市。到目前为止，已经积累了 10 多年的开发经验。

在选择企业办公平台时，我们首先要考虑两大因素，一是稳定，二是安全。目前在移动办公行业内，绝大多数的服务商都是中小型的创业公司，成立时间短，缺少稳定的收入来源，也没有相应的安全

资质，随时有可能由于经营不善而倒闭，如果企业把数据存放在这些平台上就无法得到有效的保障。

道一信息目前面向大型企业提供云定制和私有化部署服务，保证了道一信息长期稳定的资金流及营业收入，这些稳定的大型项目为企微云平台打下了坚实的基础，除此以外，道一也获得 CMMI 4 级、信息系统集成 3 级等相关认证。



在安全方面，企微云平台的开发团队在大型项目的开发过程中，积累了丰富的开发经验，也建立了极强的安全意识。在企微云平台搭建之初，就已经做了大量安全方面的工作，这些安全方面的举措也得到了权威机构的认可，比如在 2015 年道一信息就获得了 **ISO/IEC27001:2013 认证，目前只有极少数的企业号服务商获得此证书。**

1.2、ISO/IEC27001:2013 信息安全管理体系认证证书

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：15X10023R0M

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

什么是 ISO/IEC27001：2013 认证？

ISO27001：2013 认证是目前国际上最权威、最严格、也是最被广泛接受和应用的信息安全体系认证。已在世界各地的政府机构、银行、证券、保险公司、电信运营商、网络公司以及许多跨国公司得到了广泛认可，国内获得这项证书的还包括微信、阿里钉钉等。**道一信息比微信、阿里钉钉早一**

年多获得了此认证。

ISO27001:2013 认证对企微有何意义？

ISO27001：2013 信息安全管理体系的认证，证明了企微云端技术框架、内部管理矩阵达到国际信息安全的要求。企微的安全管理程序符合国际公认的标准，并通过了独立第三方审计的验证，证实了企微拥有一个系统的、科学的方法来保障自身及客户的信息安全。

1.3、企业信息安全是企微的生命线

企微始终将用户信息安全放在首位，安全是企微的生命线

企微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，也是企微能够持续稳定发展的生命线，企微投入了巨大的资源来确保用户的数据安全，因此也得到许多大型企业的认可。

用户的声音是对我们最真切的肯定

企微云平台是微信企业号最大的应用服务商，已汇聚超过 8 万多家企业、覆盖 60 多个行业，为中国移动、中粮集团、梁山公安、玉溪法院、中国电信、青岛啤酒、红星美凯龙、友邦保险等企业或机构提供服务，企微得到这些大型企业或组织机构的认可也从侧面说明了企微云平台对于用户数据有极高的安全性。

腾讯官方推荐的微信企业号应用第一品牌

腾讯对服务商的要求很高，特别是在安全方面。在微信企业号立项之初，腾讯首先邀请了当时正在研发移动办公平台的企微 ,也采纳了不少企微提出的安全建议。微信企业号上线后的近 2 年时间里，企微在信息安全和系统稳定上得到了腾讯的认可，也是腾讯推荐的微信企业号应用第一品牌。

2、企微信息安全机制

2.1 服务器安全

企微云平台部署在稳定性和安全性最强的阿里云云服务器上，企微高度重视信息安全，拥有自己的专业运维团队，同时斥巨资与国内顶级的安全厂商合作，还聘请安全专家提供信息安全方案。企微从多个层面保障企业数据的安全，服务器可抵御绝大部分的网络攻击，防止数据泄漏。

2.2 多服务器保障

企微云平台采用分布式的服务器集群。用户数据是以分布式的模式进行储存，即使某个服务器出现故障或者通讯线路受阻断，也不会影响用户的正常使用。

2.3 数据存储安全

企微云平台上所有用户的数据都会进行加密存储，以保证企业数据的安全。

2.4 数据定时备份

企微云平台配有备份服务器，系统会自动将数据备份到灾备中心，可实现自动备份，提供不间断的数据备份和恢复功能。

2.5 系统维护安全

企微的服务器配备入侵检测系统（IDS）、入侵防御系统（IPS）、系统自动巡检功能、自动预警功能，实现 7*24 小时的系统维护，同时拥有专职的系统运维人员，为企业信息安全提供全方位的保障。

2.6 系统访问安全

企微云平台建立了严格的系统访问机制和口令识别机制，非授权人员不能访问管理系统，可有效避免信息的泄漏，保障用户和企业的信息安全。

2.7 灾难防护措施

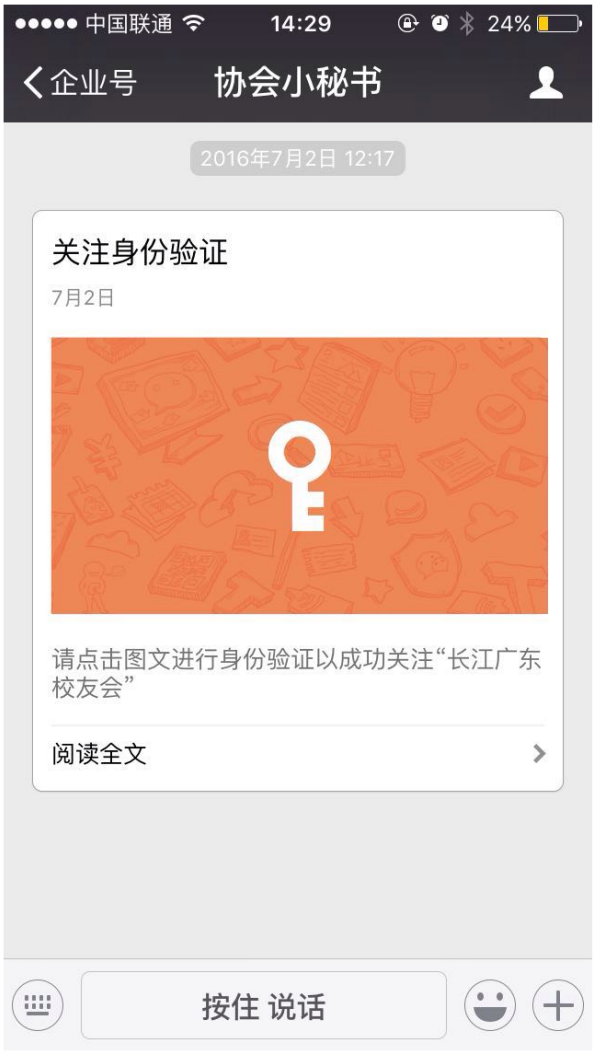
为保障平台 7*24*365 全年不间断运作，企微采用了全方位的防护措施，能确保企微云平台提供的服务不会因为电力故障、火灾、潮湿、高温等气候变化而受到影响。

3、大家都关心的企微信息安全问题汇总

3.1 企业号的安全验证机制是什么？

企业号非常重视企业的信息安全，为了让企业确保关注者都是企业许可的人员，所有关注企业号的成员都要事先进行身份验证。

企业号不像订阅号和服务号扫码就能直接关注，企业号需要管理员先把人员信息录入企业号后台，然后扫码才能顺利关注，这样就保证了非企业内部的人员不容易混进企业号。



3.2 员工离职或者调岗后，如何保障信息安全？

若员工离职，企业管理员可在通讯录中删除或禁用该成员。离职人员一旦被管理员设置为离职状态，该离职人员的企业号应用端会自动取消关注， 但是该人员之前产生的数据仍会保留。假如选择删除，则会清除该员工在企微云平台上产生的所有数据，而且这个操作不能撤销。因此，我们推荐用户使用【离职】功能管理员工。

若员工调岗，管理员可更新该成员的部门信息，此时员工在企业号里的权限也将根据管理员的设定进行调整。

3.3 员工手机丢失或账号被盗后，企业信息安全如何保障？

当员工的手机出现丢失的状况，企业号管理员可在管理后台对该员工进行禁用操作，禁用后，该员工微信上将无法再阅读或收发企业号的消息。

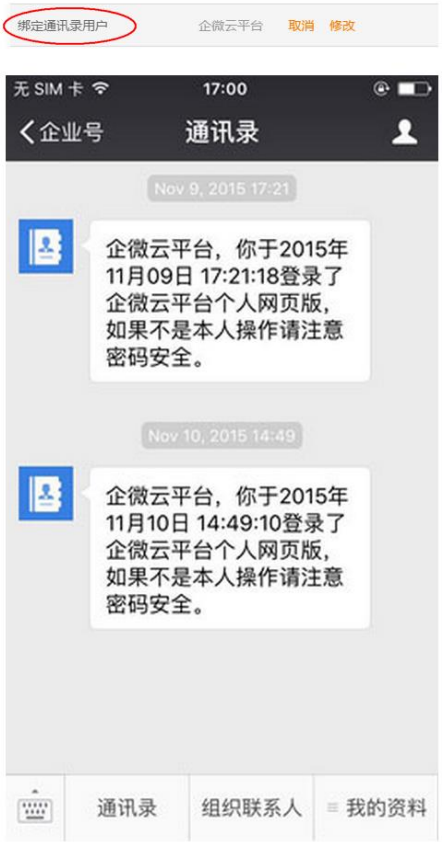
3.4 企微工作人员能看到企业的数据吗？

企微云平台上所有数据都已经进行了加密存储，企微的工作人员都无法查看。

4、企微安全防御、避免隐患措施

4.1 登录提醒

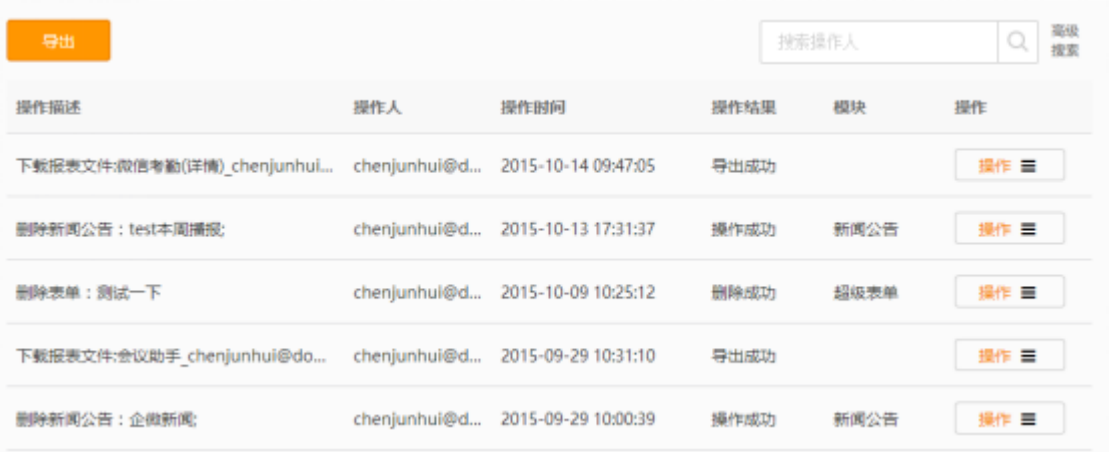
管理员账号可以与通讯录用户进行绑定（设置中心-账号信息管理），绑定后，登录管理后台时会收到登录提醒，如收到登录提醒时不是后台管理员的操作，管理员应及时处理以保障企业信息的安全。



4.2 日志查询

管理员账号交给多人个管理，如果出现问题如何查出是被操作的？

企微提供操作日志查询功能。每一条数据修改、增删等都有完整的操作日志可以查询，如发现有异常行为，可以及时查询日志，找出原因以便管理员进行处理。



4.3 权限分级

在企微云平台管理后台的【设置中心】，管理员可以分配管理子账号，满足不同部门的管理需求，避免所有的用户共用一个管理账号而出现系统管理方面的风险。比如行政部门只能使用新闻公告管理功能，那么就可以通过配置一个“行政部管理员”的角色，并对该角色赋予新闻公告的管理权限。

请点击教程查看：进阶技巧-子账户管理

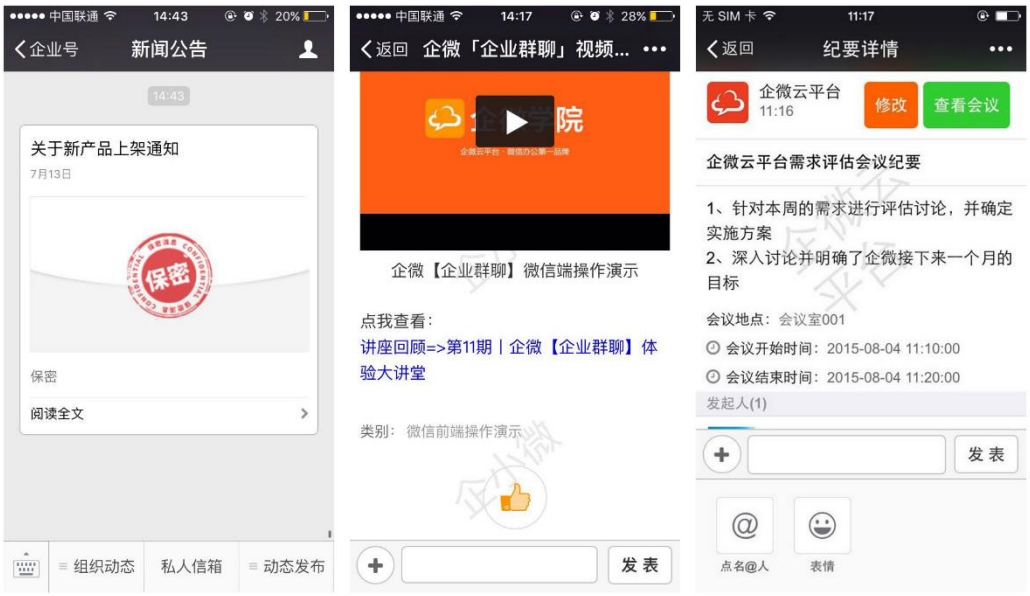
http://wbg.do1.com.cn/help/jinjiejiqiao/2015/0930/447.html

4.4 防转发、防截屏、销毁功能

防转发：非企业号成员是无法查看企业号内部文章的，因此即使有员工对外转发，外部人员也无法查看。

Tips：在部分实际使用场景下，一些内部公告及资源需要分享到外部，此时管理员也可以通过自主开启企微的【外部分享】功能，实现对外转发

防截屏：企微的新闻公告、知识百科和会议纪要，都有水印功能，开启之后，员工打开消息后会显示员工的名字水印。



销毁功能：新闻公告的私人信箱，具有销毁的功能，防止被他人拿到手机后看到企业内部信息。

5、给企微用户的一些建议

据国际安全机构统计数据显示，80%以上的信息安全问题不是来于自系统本身，而是由于人为的失误或者企业内部泄露导致的。通过一些方法可以有效地减少这类信息安全问题，帮助广大企业用户能够更好更安心地使用企微云平台。

5.1 设置复杂的管理后台登录密码

为了防止不法分子恶意破解用户登录密码，建议企业管理员采用数字、字母大小写、符号等组合，同时尽量避免设置强度低的密码，尽可能提高密码的安全级别。

5.2 定期修改管理后台登录密码

定期修改登录密码，推荐以三个月为周期设置密码，密码尽量不要跟其它平台密码重复，以提高账

号的安全性。

5.3 定期清理离职员工通讯录

在企业内部，常常会出现人员的流动，对于离职员工的账号，应该采用删除或者禁用账号的方式，保证企业号只允许内部员工访问。

5.4 员工使用企业号培训

微信企业号管理员可以适当制定一些培训措施，帮助企业员工按照正确的方式使用企业号，当遇到一些突发状况，例如手机丢失、账号被盗等情况时，应该及时通知管理员，方便管理员及时对账号进行禁用或者锁定，避免信息泄密造成损失。

6、个人密码管理

6.1 一个安全的管理密码工具

随着我们注册的账号越来越多，在不同的平台使用不同的密码，记住这些密码便成为了一个痛点，很多人都会遇到忘记密码的时候。

LastPass——安全的密码管理工具。

在浏览器安装 LastPass 这个扩展应用程序，你只需要给 LastPass 设置一个复杂的主密码，开启两步验证，通过 LastPass 记录一些账号密码，以后在登录其他平台的时候只需要记住 LastPass 的主密码就可以了。

Lastpass 主要功能：

①经常访问的网站只需一次点击，就会自动输入账号密码登录；

②同一平台多个账号可以非常方便的来切换登录；

③账号共享：让其他人使用你的账号，但是不需要将密码告诉他；

④支持 IE、360 、谷歌等浏览器，密码信息会和其他浏览器保持同步；

⑤手机上也能访问：在手机、平板等移动设备也可以登录，随时随地安全访问您的密码；

⑥多重安全机制，可有效保护账号的安全。黑客曾经攻击 LastPass 服务器，获取了一部分数据，但至少没有人说能解密这些被加密的数据；

⑦自动生成密码：能自动生成高度复杂的密码，包括符号、数字和字母大小写混写组合起来的密码。

6.2 手机安全很重要

开启 PIN 码保护手机 SIM 卡的安全

开启手机 SIM 卡 PIN 锁后，把手机卡安装到另外一部手机时，会提示需要输入 PIN 码，如果没有输入正确的 PIN 码，就无法正常使用此手机卡，输入错误 PIN 码超过一定的次数，SIM 卡会被锁定，这样就可以避免手机丢失时，别人通过手机卡来修改我们的支付宝、网银等重要账号。如果手机重启后，也需要输入 PIN 码才能正常使用手机 SIM 卡。如果忘记 PIN 码，可以通过登录运营商官网进行重置。

注意：设置 PIN 码请慎重并记住！近期发现电信手机输入 PIN 码 3 次出错被锁住后，无法用 PUK 码解锁的情况。

6.3 重要的邮箱开启两步验证

对于注册账号时关联的重要邮箱，推荐使用谷歌邮箱，或者使用 outlook 这种可以开启两步验证邮箱。开启两步验证之后，即使我们的邮箱账号密码被盗取了，也无法获得我们手机里面的动态验证码，这样就无法通过邮箱来找回其它平台的账号和密码。

6.4 手机尽量不 Root、不越狱

当手机被 Root（或越狱）之后，也就等于敞开了系统最高权限的大门，很容易被恶意的程序利用。如果手机本身不安全，其它安全措施就形同虚设，为了手机的安全建议不要 Root（或越狱）。

6.5 扫码安全登录

在网吧等公共场所或临时使用其它人的电脑，需要使用 QQ、淘宝时，最好使用扫码登录。

6.6 良好的使用习惯很重要

尽可能养成良好的使用习惯，应该从官方渠道下载软件，避免随意连接一些陌生 WIFI，以免手机中的个人隐私等信息被恶意窃取。

6.7 安全意识不能忘

生活中多注意使用信息处理的细节，可以大大降低账号密码被盗的风险，但是现在网络环境越来越复杂，多学习了解一些网络安全的知识，有利于个人的切身利益，保护我们个人的信息安全。

Part Two：精选问答

问题 1.企业收付款安全问题？

答：在支付方面，我们是直接调用腾讯微信的提供的支付接口。微信与保险公司有合作，为用户推出全额赔付的保障，用户如因使用微信支付造成资金被盗等损失，将可获得保险公司的全赔保障。如果出现支付不到账或支付后出问题的情况，可以与我们工作人员取得联系。

问题 2.保密文件的转发记录后台是否能调取到，用于风险爆发后的排查等？

答：对于保密文件，在新闻公告、百科和会议纪要中，有开启水印功能，员工在微信端打开页面详情时会显示姓名水印，风险爆发后可排查。另外，对于一般文件员工转发给其他人，非企业号内部的人是看不到。

问题 3.不是负责人和相关人，能看到数据吗？

答：是不能看到的。你提交的内容，想给谁看，就把谁设置为负责人或相关人，其他人是看不到的，会提示“没有权限访问本页面”。

问题 4.通讯录授权后，会不会信息泄漏，可以授权部分通讯录吗？不从根目录授权。

答：若是不从根目录授权，会导致数据交互问题的。另外，授权只是授权账号和部门的信息，不用担心。企微云平台的信息安全高度与腾讯也是保持一致的，企业的信息安全问题是我们最为重视的问题之一。

问题 5.企微通讯录权限方面，有部分员工需要分配“所有人”的权限，但又不想让其看到所有人的通讯录，应该如何处理？

答：这个可以通过企微设置通讯录查看权限，具体如何设置可以看一下教程。

通讯录操作手册：http://wbg.do1.com.cn/help/work_suite/2015/1012/479.html

问题 6.所有的人事档案搬进来了之后，人事资料的安全问题。

答：人事资料的安全跟其他数据的安全是一样的，都是加密存储的。

问题 7.考勤如何更精确定位？

答：企微考勤轮，可以实现更精确的定位，可以点击下方链接购买。

【签到神器】颠覆传统考勤，深扒新一代智能办公硬件：http://t.cn/RtwujwF

问题 8.据说阿里云的用户使用协议授权阿里读取用户数据，请问有什么说明解释吗 ？

答：没有和阿里对接接口，阿里的授权是在微信企业号体系建立起来才发布的，和微信的比较相似。

问题 9.用户登录可以与我公司的密码验证体系集成吗？

答：每个公司的密码验证体系不一，可以通过定制开发实现与自有业务的验证体系集成。

问题 10.企微能免费多久使用？

答：企微云平台开放的 7 大套件 25+个基础应用永久免费使用，并会提供一些付费增值服务，企业可以选择是否使用增值服务（增值服务不影响免费基础应用的使用）。对于中大型企业，提供企微产品独立部署、个性化需求定制等收费服务。

问题 11.如何给发布的链接加背景音乐和动画图片？

答：可以看一下教程哦！【企微实用技巧】插入图片、视频及音乐，让你的『动态』更有看点：http://t.cn/Rtwz0ow

问题 12.如何修正考勤定位错误信息比如员工实际签到是 a 大街 100 号，但微信确显示 b 大街 90 号？

答：微信的位置是做了等待 GPS 定位返回数据，但是微信提供的接口是不会等待 GPS 返回准确的定位信息，因此会造成微信分享出来的位置准确，而应用签到通过微信接口获取的位置不准确的问题。如果遇到这个问题，切换网络签到或请多试几次应该可以解决。如果需要特别精准考勤，也可以考虑使用考勤机，可以指纹或是刷脸考勤。

问题 13.能否新增文件共享功能，并整合到私有云端或 NAS 里（类似电信私有云空间、NAS 网络存储器）。场景：人事部表单模版、党建表单模版，需要相关员工填写完之后再直接存档到本地 NAS 网络存储器或电信私有云空间，可以手机直接操作完成，流程中可见方始终是部门与个人，其他人无权随意查阅。

答：这些表单模板可以用企微的超级表单来制作，并设置查阅权限，实现你想要的功能。若是要整合到私有云的话，需要定制，请讲座结束后联系我们的工作人员。

超级表单操作指南：http://wbg.do1.com.cn/help/WX_suite/2015/1012/478.html

问题 14.可以设置某些个别员工的手机号不被其他员工看到吗？比如说企业特聘的一些人员，防止号码泄露友商挖墙脚的。

答：可以在企微通讯录中，不输入此特聘成员的手机号码，则无法查看到此成员的手机号。也可以在企微通讯录-设置中，将手机号码设置为不显示，则企业通讯录中所有成员都不显示手机。

活动回顾到此结束，非常感谢大家对于企微云平台的支持

我们下一次企微大讲堂再见！