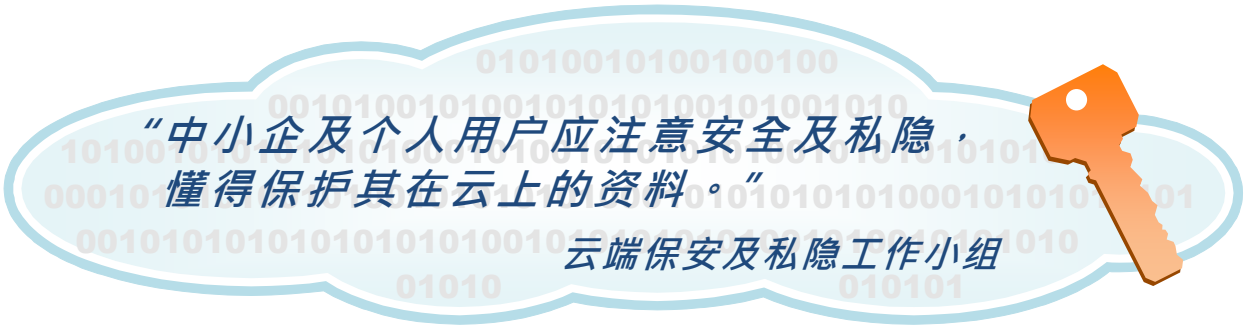
云用户
的信息安全备忘事项



目的

云服务无远弗届、方便使用、具成本效益，故愈来愈多工商机构及个别人士使用。本文件载列了信息安全方面的三份备忘事项，以供用户在考虑使用或在使用云服务时参考。

目标对象

本文件的主要目标对象是云用户，包括中小型企业（下称“中小企”）及个人用户。

讨论范围

本文件的重点集中在云用户服务上，当中涉及用户储存及分享自己的资料；以及经互联网或其他网络连接方式，连接第三方服务提供商拥有或营运的远端服务器，从而使用已安装的云应用程序。当使用这些云服务的基本功能时，一般都是免费的，但一些进阶服务则可能须向用户收取费用。云服务的例子包括网上电邮、社交网站、资料储存、照片分享网站、联络人管理、文件管理及其他应用程序。这些服务通常属“软件即服务”，即透过寄存在中央云上的软件提供服务，而相关资料，亦会寄存在中央的云上。

云用户关注的安全问题

很多人因担心服务中断、资料遗失、私隐、帐户遭黑客入侵和法例问题而对使用云服务有戒心。对熟悉应用信息技术的企业而言，他们很可能具备技术和资源，以监察服务提供商的服务水准，评核服务提供商是否符合安全规定，或自行采取额外安全措施保护其资料。

另一方面，一般云用户及中小企用户可能忽略本身的权利及责任，也可能不清楚如何选择可信靠的云服务提供商，以及可能不肯定在使用云服务时，其资料是否充分受到保护。

云用户应注意哪些事项？

云用户透过云处理或储存的资料，可能包含有价值、敏感和牵涉个人的资料。用户要保护这些资料，单靠云服务提供商所采取的安全措施并不足够。对中小企用户而言，他们需要懂得在选择云服务提供商和使用云服务时要考虑什么安全措施。对所有云用户（包括商业和个人用户）而言，他们需要深入了解在云上保护其资料所遇到的困难和考虑。

中小企在选择云服务提供商的备忘事项

服务条款及安全和私隐政策

- 中小企公司须阅读服务提供商的服务条款及安全和私隐政策，并应注意：
  - 公司可如何使用云服务（即使用限制条款、使用权或使用限制）；
  - 资料是如何储存及受到保护；
  - 服务提供商是否可以存取你的公司资料。如果可以的话，此类存取是怎样被限制的；
  - 如何举报安全事故；
  - 如何终止服务，以及在终止服务后，如何处理仍然保留在相关云上的资料；
  - 服务提供商会否在更改服务条款前预先发出通知；
  - 私隐政策是否遵从《个人资料（私隐）条例》[1]的保障资料原则；以及
  - 条款可适用于哪些司法管辖区（香港特别行政区或其他地区）。
- 如不接纳某些服务条款，应与服务提供商洽谈。如物色不到能够满足所订要求的服务提供商，应重新考虑是否需要使用云服务。
- 了解帐户资料会否在用户不知情或未经用户同意的情况下作“次要用途”，例如储存在云上的资料可能会被用来制作切合用户需要的广告。

资料拥有权

- 查核服务提供商是否保留权利，可使用、披露或公开用户所拥有的资料。
- 查核用户能否保留所拥有资料的知识产权。
- 查核即使资料从云上被删除后，服务提供商会否保留使用该些资料的权利。
- 了解用户能否按本身意愿把资料及服务转移至另一服务提供商，以及是否有容易用的资料汇出功能供用户使用。
- 从云上删除资料或停止使用该服务时，应检查这些资料（包括任何储存备份资料）是否可被永久删除。

选择服务提供商时的其他考虑因素

- 了解使用云服务所涉及的风险和公司可接受的风险程度。
- 选择服务水准协议与你的业务重要性相符的服务提供商。
- 选择能清楚说明提供哪些安全功能的服务提供商，有独立信息安全管理认证（例如ISO/IEC 27001）者为佳。
- 选择不曾发生重大安全事故，或即使曾发生安全事故但能清楚解释事发原因及补救办法的服务提供商。
- 选择能透过以下途径确保用户资料得以保密的服务提供商：
  - 使用加密功能（例如安全套接层(SSL)）以传送资料；以及
  - 使用加密功能以保护储存资料。（如供应商没有提供加密功能，用户应自行为资料加密，然后才储存在云上，并须安全保管用以加密的密钥。）
- 选择设有简单清晰通报机制的服务提供商，以供举报服务问题、安全事故和侵犯私隐事宜。
- 选择能定期提交服务管理报告及安全事故报告的服务提供商。

中小企在使用云服务的备忘事项

身分识别和认证

- 如云服务有提供的话，应使用严谨的认证方式，例如双重认证，用户可以使用其本人的特征（例如指纹）、拥有的凭证（例如数字证书）和所知的资料（例如密码）的其中两项进行认证。
- 帐户应使用难被猜中的密码。
- 不同的帐户应使用不同的密码。
- 不同的员工应使用不同的帐户。
- 定期更改密码。
- 出现人事变动时，应即时删除有关用户帐户或更改密码。

云管理

- 就云服务的使用制订一套简单的帐户政策。
- 制订简单的使用政策供员工遵守。
- 指派一名合适的员工（对云服务有基本认识）担任云服务管理员。
- 定期检讨员工对云上资料所拥有的存取权。
- 为使用云服务的员工提供基本安全认知培训。

资料保护

- 了解并记录储存于云上资料的种类。
- 遵从《个人资料（私隐）条例》[1]以保护个人资料。
- 透过以下途径避免把资料分享给非预定人士：
  - 如用户拟透过云上与他人分享敏感资料，确保只有指定收件人才可存取；
  - 确保任何运行于用户装置用作连接云服务的应用程序，只可把有关装置与云之间的许可资料同步；以及
  - 替档案或文件夹预设合适的存取权限。
- 了解资料(包括备用副本)的储存位置(及所属司法管辖区)，并评估不同的法规遵行要求对安全程序是否有影响。

服务的持续性

- 向服务提供商索取有关服务支援的联络资料(特别是保存可以用作通报计算机安全事故的电话号码清单)。
- 评估云服务中断、资料遗失或资料被他人擅自存取对公司造成的潜在损害。
- 制订持续业务运作计划和替代方案，以应对云服务停用或资料不能被读取的情况。
- 拟订退出策略，确保有关终止程序允许把资料传送回公司。
- 定期为储存在云服务中的资料备份。
- 为重要资料进行备份至公司，即使服务提供商暂时(例如网络发生故障)或永久不能提供服务，有关资料仍可供使用。

个人用户在云上保护其资料的备忘事项

服务条款及安全和私隐政策

- 个人用户须阅读服务提供商的服务条款及安全和私隐政策，并应注意：
  - 资料是如何储存及受到保护；
  - 如何举报安全事故；以及
  - 如何终止服务，以及在终止服务后如何处理仍然保留在相关云上的资料。
- 如不同意服务条款和政策，可以不使用有关服务。应留意服务条款和政策定期作出的修订。

资料保护

- 审慎考虑是否必需把敏感资料储存于云上，并评估这些资料一旦披露所造成的影响。
- 避免在不确定对方身分的情况下分享资料，做法如下：
  - 如用户拟透过云上与他人分享敏感资料，应确保只有指定收件人才可存取；
  - 确保任何运行于用户装置用作连接云服务的应用程序，只可把有关设备与云之间的许可资料同步；以及
  - 检查使用中的档案或文件夹的预设存取权限是否合适。例如，一个预先安装的“图片”文件夹可能被预设为开放任由他人存取，这种设定不利于资料保护。
- 为重要资料进行备份至公司，即使服务提供商暂时（例如网络发生故障）或永久不能提供服务，有关资料仍可供使用。
- 透过以下途径确保服务提供商令资料得以保密：
  - 使用加密功能（例如安全套接层(SSL)）以传送资料；以及
  - 当储存资料时，使用加密功能。（如供应商没有提供加密功能，用户应自行为资料加密，然后才储存在云上，并须安全保管加密密钥。）

登入帐户安全[2]

- 帐户应使用难被猜中的登入密码。
- 不同的帐户应使用不同的登入密码。
- 透过下列方法保护用户名称及密码：
  - 放在安全的地方；
  - 避免与他人分享；
  - 关闭浏览器和应用程序的密码储存功能；以及
  - 避免以纯文字方式把密码储存于设备上。
- 确保以上安全措施实施在任何运行于计算机或移动设备上用作连接云服务的应用程序。
- 当完成工作后，登出云服务。

存取设备安全[3]

- 只使用可信靠的存取设备连接云服务。切勿使用公用计算机处理云上的敏感资料。
- 保护存取设备免被他人擅用。
- 启动计算机或移动设备的屏幕锁定功能。
- 切勿破解存取设备（即移除生产商所设定的使用和存取限制）。
- 定期为计算机及移动设备的操作系统、浏览器和计算机应用程序进行更新和安装最新的安全修补程式。
- 小心谨慎浏览互联网，特别不要点击来历不明的连结。

参考资料

1. 参考 http://www.pcpd.org.hk/chinese/ordinance/ordglance1.html#dataprotect
   有关《个人资料(私隐)条例》的保障资料原则
2. 参考 http://www.infosec.gov.hk/sc_chi/yourself/account.html
   有关帐户及密码的处理
3. 参考 http://www.infosec.gov.hk/sc_chi/virus/geninfo_common.html
   有关保护你的计算机从而更有效地对抗计算机病毒与恶意代码攻击的最佳作业实务

「云资讯网」是一站式入门网站，由云端运算服务和标准专家小组建立，方便市民和企业（特别是中小企）有效取得有关云计算技术的信息和资源。該網站提供用例、相关指引和良好作业模式，让市民和企业在采用云计算模式时达到预期效益。

云端运算服务和标准专家小组由香港特区政府属下的政府资讯科技总监办公室成立，透过广纳业界、学术界、专业团体及政府的专业知识，推动香港云计算的应用和发展，以及促进本港云计算专家彼此交流及与内地专家互相交流。云端保安及私隐工作小组是一个在专家小组辖下设立的工作小组。

此文件由云端保安及私隐工作小组发表，载述了有关云安全及私隐的良好作业模式和指引。工作小组成员透过通力合作，制订有关措施，以推动并促进本地业界，更广泛应用云计算和安全使用云服务。