政府资讯科技总监办公室

信息安全

社交媒体安全

实务指南

第 1.1 版

2021 年 6 月

版权公告

修改记录				
修改次数	修改详情	经修改页数	版本编号	日期
1	增加关于个人资料保护的安全风险及措施建议；更新常见社交媒体平台的安全提示的网址。	8; 14; 16-19; 21-22	1.1	2021 年 6 月

目录

1. 简介

不论是个人或商业用途，社交媒体都越来越受欢迎。正确使用社交媒体可以改善公众形象，成为有效的宣传工具。另一方面，使用社交媒体也存在不少安全风险。各决策局 / 部门在使用社交媒体作为与公众沟通的官方工具时，应小心谨慎，评估风险，并采取适当的保护措施。

1.1 目的

本实务指南旨为各决策局 / 部门提供通用的安全考虑和良好作业模式，以管理和使用社交媒体。本文件第 4 节描述使用及管理社交媒体的良好作业模式。社交媒体是一种基于互联网的应用。故此，用户需要正确使用互联网，以保障信息技术环境的安全。有关互联网安全的考虑因素，请参阅**附件 B**。

本文件应按需要与其他安全文件如《基准信息技术安全政策》[S17]、《信息技术安全指南》[G3] 及相关程序和指引一同使用。

1.2 参考标准

以下参考文件为本文件在应用上不可或缺的参考：

- 香港特别行政区政府《基准信息技术安全政策》[S17]
- 香港特别行政区政府《信息技术安全指南》[G3]
- Information technology – Security techniques – Information security management systems – Requirements (second edition), ISO/IEC 27001:2013
- Information technology – Security techniques – Code of practice for information security controls (second edition), ISO/IEC 27002:2013

1.3 定义及惯用词

本文件将会采用《基准信息技术安全政策》和《信息技术安全指南》内所使用，以及以下的定义及惯用词。

缩写及术语	
不适用	不适用

1.4 联络方法

本文件由政府资讯科技总监办公室编制及备存。如有任何意见或建议，请寄往：

电邮： it_security@ogcio.gov.hk

Lotus Notes 电邮：IT Security Team/OGCIO/HKSARG@OGCIO

CMMP 电邮： IT Security Team/OGCIO

2. 信息安全管理

信息安全是关于安全控制和措施的规划、实施和持续提升，以保护信息资产的机密性、完整性和可用性，适用于信息的存储、处理或传输过程及其相关信息系统中。信息安全管理是一套有关规划、组织、指导、控制的原则和应用这些原则的法则，来迅速有效地管理实体、财务、人力资源和信息资源，以及确保信息资产和信息系统的安全。

信息安全管理涉及一系列需要持续监测和控制的活动。这些活动包括但不限于以下的范畴：

- 安全管理框架与组织；
- 管治、风险管理和遵行要求；
- 安全操作；
- 安全事件和事故管理；
- 安全意识培训和能力建立；和
- 态势感知和信息共享。

安全管理框架与组织

决策局 / 部门须根据业务需要和政府安全要求，制定和实施部门信息安全政策、标准、指南和程序。

决策局 / 部门亦须界定信息安全的组织结构，并为有关各方就安全责任提供清晰的定义和适当的分配。

管治、风险管理和遵行要求

决策局 / 部门须采用风险为本的方法，以一致及有效的方式识别信息系统的安全风险、订定应对风险的缓急次序和应对有关风险。

决策局 / 部门须定期和在必要时对信息系统和生产应用系统进行安全风险评估，以识别与安全漏洞相关的风险和后果，并为建立具成本效益的安全计划和实施适当的安全保护和保障措施提供依据。

决策局 / 部门亦须定期对信息系统进行安全审计，以确保当前的安全措施符合部门信息安全政策、标准和其他合约或法律上的要求。

安全操作

为保护信息资产和信息系统，决策局 / 部门应根据业务需要实施全面的安全措施，涵盖业务上不同的技术领域，并在日常操作中采取「预防、侦测、应急和复原」原则。

- 预防措施避免或阻止不良事件的发生；
- 侦测措施识别不良事件的发生；
- 应变措施是指在发生不良事件或事故时，采取协调行动来遏制损害；和
- 复原措施是将信息系统的机密性、完整性和可用性恢复到预期状态。

安全事件和事故管理

在现实环境中，由于存在不可预见并致服务中断的事件，故此安全事故仍可能会发生。若安全事件危及业务的连续性或引起数据安全风险，决策局 / 部门须启动其常规安全事故管理计划，以实时识别、管理、记录和分析安全威胁、攻击或事故。决策局 / 部门亦应准备与有关各方适当地沟通，透过分享对有关安全风险的应变以消除不信任或不必要的猜测。当制定安全事故管理计划时，决策局 / 部门应规划和准备适当的资源，并制定相关程序，以配合必要的跟进调查。

安全意识培训和能力建立

因为信息安全每个人都有责任，所以决策局 / 部门应不断提升机构内信息安全意识，透过培训及教育，确保有关各方了解安全风险，遵守安全规定和要求，并采取信息安全的良好作业模式。

态势感知和信息共享

因应网络威胁形势不断变化，决策局 / 部门亦应不断关注由安全行业和政府电脑安全事故协调中心发布的现时安全漏洞讯息、威胁警报和重要通知。应将即将或已经发生具威胁的安全警报传达及分享给决策局 / 部门内的负责同事，以便采取及时的应对措施来缓解风险。

决策局 / 部门可以使用网络风险信息共享平台来接收和分享有关安全问题、漏洞和网络威胁情报的信息。

3. 社交媒体概述

3.1 社交媒体介绍

社交媒体是指参与者在互动平台上进行互相交流。近年来，社交媒体被普及使用。起初，Facebook、Instagram 和 YouTube 等社交媒体平台的用户建立具有共同兴趣的朋友网络。现在，它不仅用于个人分享，还用作为商业或政府的沟通渠道，与公众或目标观众互动和合作，以征求意见和看法。然而，在网络安全方面，这可带来一定的相关风险。

在政府内部，参与社交媒体的决定应该由运作需求主导，并得到管理层的支持，亦应考虑到范围、威胁、技术能力和潜在利益。为了抵御社交媒体迅速发展的威胁，应制定风险管理方案，以评估风险并将其降低到可接受的水平。在保护参与者、平台和服务以及政府人员和资料方面，应考虑采取纵深防御的缓解措施[1]。

3.2 常见社交媒体类别

随着社交媒体的日益普及和强大，用户享受社交媒体平台所带来的不同网络的好处。以下是用户广泛使用的常见社交媒体类别。

社交网络

- 社交网络使用户可以与其他用户和品牌在线联系，并鼓励知识共享，实现人与人之间的互动。

媒体分享平台

- 媒体分享平台使用户可以分享各种视觉内容，如影片、图像、信息图和插图。与社交网络不同的是，这平台着重于分享视觉内容，并经过优化以帮助创作者上载其视觉内容并与其他观众互动。

[1]纵深防御是透过利用分层保护和控制措施的方法，以保护信息系统和数据。

论坛和社交小区

- 论坛和社交小区是指人们可以通过发布信息的形式进行对话，以获得集体知识的在线讨论网站。用户可以匿名，也可以在论坛上注册一个用户名称，然后再发布信息。

博客网络

- 博客网络使用户和公司可以在在线发布内容，帮助提高让观看者发现发布内容的可见性。这种类型的社交媒体通常用于建立参与度，让人们熟悉博客。

4. 社交媒体安全风险与威胁

决策局 / 部门应制定风险管理方案，以了解威胁并评估社交媒体参与者、平台和服务，以及决策局 / 部门（即订户）和所涉及的资料的相关风险。

- 参与者：一般公众用户，如参与社交媒体平台的公众。
- 社交媒体平台和服务：让政府和公众互相沟通、协作、互动和分享信息的网上媒体平台。
- 决策局 / 部门：商业或公共服务提供商的社交媒体服务的订户。

4.1 对社交媒体参与者的威胁

社交媒体平台存在与公众参与者（例如在论坛发布讯息的市民）相关的安全威胁。安全威胁包括私隐威胁、丢失登入凭证、恶意内容和程序代码、社交工程攻击等。

私隐威胁

社交媒体，如论坛和博客，容许参与者向公众发布信息或内容。这些交流形式可能因放置过多个人资料而带来私隐问题，平台或容许根据个人行为而制作个人档案，并作出对用户不利的决定。如果参与者在社交媒体平台上发布过多个人资料，可能会对参与者造成潜在的不利局面。这此资料会留下永久的数码足迹，难以从网络世界中移除，而且或会被滥用于身份盗用。

被盗或丢失登入凭证

如果密码拣选不当或保护不当，恶意者会设法盗取密码。如在未经授权下登入账户，恶意者可能会发布假冒讯息或利用帐户传播恶意软件。

恶意内容、程序代码和仿冒诈骗连结

由于用户数量和发布个人信息的数量众多，社交媒体已成为其中一个攻击向量而此攻击亦逐渐普遍。攻击者可能会利用这渠道传播恶意内容、程序代码或仿冒诈骗连结。如果社交媒体网站存在安全漏洞，攻击者能编写看似正常的应用程序，使计算机在用户不知情的情况下受到感染。

社交工程攻击

社交媒体建立具有一定人际信任度的网络小区。恶意者可冒充用户信任的人，并说服他们披露敏感资料。此外，在使用一些社交工程技能时，攻击如病毒、特洛依木马或谣言等能容易地和迅速地传播。

4.2 对社交媒体平台和服务的威胁

对于社交媒体平台和服务存在的威胁，如服务供货商提供的论坛、博客和实时通讯等。就威胁的影响而言，平台的正常运行可能会受到干扰、服务可能会被中断，以及资料可能会被未经授权的存取和披露。

以下是对于社交媒体平台和服务的常见威胁：

缓冲区满溢

缓冲区满溢是一种广为人知的软件安全漏洞。在经典的缓冲区满溢漏洞，攻击者将数据发送到程序，而程序将其存储在一个容量过小的堆栈缓冲区。结果是呼叫堆栈的资料被盖写，当中包括函数的返回指针。由于数据设置返回指针的价值，所以当函数返回时，会把控制权转移到攻击者数据中包含的恶意代码。

远程代码执行漏洞

攻击者利用漏洞执行恶意代码，并利用用户的权限完全控制受影响的平台 / 系统。在访问平台 / 系统后，攻击者会试图提升其权限。

滥发邮件

滥发邮件是针对社交媒体网站传播垃圾邮件的常见攻击方式。它滥用电子讯息系统，大量发送未经请求的讯息。论坛滥发邮件是指那些辱骂、营销噱头、或是无用的信息。在论坛没有管理的情况下，滥发邮件可以频繁地发生。它可能在短短几个小时，甚至几分钟内发生，甚至可能由于信息泛滥而导致论坛服务器停止服务。这将消耗资讯系统的资源，并对其他正常服务的服务水平产生负面影响。更重要的是，参与者可能会发现社交媒体平台上充斥着无用的信息，并且对参与进一步的讨论失去兴趣。

网上应用程序攻击

网上应用程序是使用动态网页为参与者提供额外的功能。然而，这些额外的功能可能意味着有更多攻击网上应用程序的机会。这使社交媒体网站为攻击者开启了可利用的广泛安全漏洞。攻击者可通过键次登入器以捕捉用户的键击，包括帐户用户名称和密码。若个人社交媒体帐户被劫持或会令人感到烦恼、尴尬甚至付出

代价，而当政府官方帐户被劫持时，可能会带来更严重的影响。非官方帖子或讯息可能被公众视为官方讯息，或可被用于传播恶意软件，使用户在不知情下点击链接或下载不需要的应用程序。

以下是一些常见的网上应用攻击的例子：

- 无效身份认证
  与身份认证和对话管理相关的应用功能经常被错误地推行，允许攻击者破解密码、密钥或对话权标，或利用其他应用程序的缺陷，暂时或永久地冒充其他用户的身份。

- 无效访问控制
  访问控制是指控制信息或存取功能的系统。无效访问控制允许攻击者绕过授权，并扮演管理员等特权用户以同等特权执行任务，例如一个网上应用程序允许用户在没有任何其他验证的情况下，只需更改统一网址的一部分，就可更改他们所登录的帐户。

- 敏感资料泄露
  许多网上应用程序和应用程序界面没有适当地保护敏感资料，如金融、医疗和个人可识别讯息。攻击者可能会窃取或修改受较弱保护的资料，以进行信用卡欺诈、身份盗窃或其他犯罪行为。敏感资料可能会在没有额外保护的情况下被泄露，例如资料在没加密的储存或传输过程中，因此在使用浏览器时需要特别的预防措施。

- 跨站脚本
  跨站脚本是一种网上应用程序攻击，诱使终端用户的网页浏览器执行恶意代码。恶意代码可能会窃取终端用户的个人资料，从而攻击者可冒充终端用户，操纵终端用户的计算机，在受害者不知情的情况下，发起攻击。

- 跨站请求伪造
  跨站请求伪造是一种网上应用程序攻击，导致终端用户的网页浏览器在用户不知情的情况下，执行攻击者选择行动。通过在网页中嵌入恶意链接或通过电子邮件或聊天发送连结，攻击者可能导致网上应用程序的用户执行不必要的行动。更具体地说，攻击者导致用户的浏览器在用户或网站不知情的情况下，向已通过验证的网站发出请求。这些行动可能损害终端用户的资料和操作，甚至令到整个服务器或网络受损。

- 注入攻击
  社交媒体使用的技术使其容易受到注入攻击，例如可扩充标记语言和结构化查询语言的注入。此外，社交媒体应用程序通常依赖于客户端代码，因此它们严重依赖于攻击者可绕过的客户端输入验证。

不恰当或具侵犯性的内容

参与者可能会在社交网站上发布或上传不恰当或具侵犯性的内容。内容可能包括未经版权授权的材料、社会普遍未能接受的道德标准或范围、有关网络攻击或药物使用等。发布这些内容可能影响政府形象。另一个顾虑是持有这些不合法内容的最终责任。

未经授权的内容变更或服务中断

在线破坏行为涉及对在线资产的损害或破坏，可能影响政府形象和声誉。行为范围从网址篡改到服务中断。

仿冒诈骗

仿冒诈骗是一种针对特定用户或用户群组的有效攻击，欺骗用户执行会发起攻击行动的行为，例如打开文件或点击连结。仿冒诈骗者依靠了解目标的个人资料，例如兴趣、旅行计划、社交圈子等。大多数时候，个人资料只是通过在社交媒体上来收集。仿冒诈骗者利用社交媒体作为另一种方式发送诈骗讯息，因为社交媒体平台绕过传统电子邮件安全控制。仿冒诈骗者在社交媒体上发布的链接可能看似正常网站，而在拼写上有些微变化，或者使用不同网域欺骗用户。

可用性和效能

由于硬件或软件问题，可能会出现服务中断的情况，或者系统容量达到极限，导致效能下降。如果发生灾难，服务可能完全无法使用，业务连续性将受到影响。另外，服务供应者（或其承包商）可能会倒闭，或在发生纠纷时挟持资料。服务供应者（及其承包商）的可信度、可靠性和能力对确保社交媒体服务的持续是非常重要。

4.3 对决策局 / 部门和资料的威胁

在网站上提供社交媒体平台的服务，将具有容易接触大量参与者的优势。因此，公共社交媒体平台往往是以社交媒体为目的而部署。不论在内部基础设施上部署，或是外判至服务供应者，这些都会令政府人员和资料受到威胁。

以下是特别针对政府人员和资料的常见威胁：

披露内部 / 保密资料

敏感或保密资料可能有意或无意地被披露，使政府声誉受损或陷入尴尬。

保留和销毁资料

各种原因可能导致决策局 / 部门与服务供货商终止协作，例如技术转变、普及程度、合约期届满及未能续约。在这些情况下，决策局 / 部门无法从社交媒体平台取回所有资料可能会导致出现数据遗失风险。另一方面，服务供应者可能没有依照适当程序弃置政府资料。

资料不正当使用

社交媒体供应者可能没有充分保障用户或参与者的私隐，以确保资料不会被用作其他用途及不可向第三方披露。服务供货商可能会收集参与者的登记资料作市场推广用途，这在一定程度上，可能会对参与者造成滋扰。

对服务和资料的有限控制

根据社交媒体服务的订购协议，资料通常在云端环境下储存和处理。在该环境下，对平台甚至政府资料的控制可能受到限制。例如，你可能无法要求对整个硬盘进行影像备份，因为它包含其他订购者的资料。

缺乏意识

缺乏意识可导致不同程度的安全漏洞。社交工程攻击可能针对政府人员，其中负责人员如社交媒体管理员可能被欺骗而泄露身份资料。此外，员工可能会在社交媒体上发布内部或保密资料，影响政府形象。

假冒

假冒者往往在社交媒体上建立类似名人、商业机构或政府官员的帐户。一些假冒他人的帐户可能带有欺骗意图，给公众传达误导性的讯息，以收集信息或获取财务利益。

5. 社交媒体安全措施和控制

5.1 社交媒体使用生命周期

5.1.1 提供社交媒体帐户

各决策局 / 部门在考虑采用社交媒体时，应确定使用社交媒体的需求，以及社交媒体如何支持其业务。决策局 / 部门应制定使用社交媒体的政策，清楚订明使用社交媒体服务的业务和安全要求。

5.1.1.1 建立社交媒体帐户

根据使用情况和安全要求，各决策局 / 部门应制定适当的流程和程序以提供社交媒体帐户。特别是，社交媒体帐户的安全配置应按照政府的安全要求执行。有关强化安全的样本配置，请参阅**附件 A**。

各决策局 / 部门应从高层管理人员中委任一名人员担任社交媒体帐户管理员主管，以及最少两名人员担任社交媒体帐户管理员，为决策局 / 部门设立、访问和管理社交媒体帐户。

管理员应建立、命名和组建代表政府或决策局 / 部门的社交媒体帐户，并提供已得到管理员主管批准的信息。这些信息包括但不限于：

- 帐户说明
- 业务信息
- 联系方式（如电邮地址、网站）
- 地址
- 个人头像的照片
- 一般信息

5.1.1.2 社交媒体使用政策

为了规范管理员和用户对社交媒体的使用，应制定适当使用社交媒体的安全政策。不同领域的社交媒体平台的常见安全和控制措施，包括但不限于：

- 一般管理
- 帐户
- 密码
- 安全设定
- 发布
- 网络和端点
- 意识

社交媒体服务的安全使用细节列于**第 5.2 节 – 安全使用社交媒体服务**。

5.1.1.3 使用社交媒体分析

社交媒体分析是在社交媒体平台收集和分析数据的过程。收集的信息包括但不限于：

- 在社交媒体平台上分享的个人资料（如个人档案资料、内容、使用情况以及第三方网站和应用程序）。
- 设备信息（如设备识别号码、属性、操作、信号、网络和连接以及小型文本文件数据）
- 来自第三方伙伴和服务的信息，包括广告商和应用开发商（如帐户资料、用户设置和社交互动活动）。

决策局 / 部门应参考个人资料私隐专员公署出版有关网上行为追踪的资料单张。

- 网上行为追踪 (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/online_tracking_c.pdf)

社交媒体分析工具帮助用户了解观众以及他们如何与社交媒体页面中的帖子互动。它提供关于社交媒体帐户的见解、指针和仪表板，包括但不限于：

- 追随者数量
- 追随者的年龄层
- 帖子的观众参与度
- 追随者访问社交媒体页面的时间和地点
- 社交媒体页面上的帖子数量
- 内容曝光次数
- 读取内容的人数
- 与内容进行互动的人数（如喜欢、分享、转发、回复或提及）

社交媒体帐户管理员应该利用社交媒体分析技术，提供更好的服务，并与社会各界互动。

5.1.2 停用社交媒体帐户

各决策局 / 部门应定期检视社交媒体的使用情况。如社交媒体帐户超过六个月没有使用，管理员应考虑停用该帐户。社交媒体帐户管理员主管亦应将此事呈报至决策局 / 部门的高级管理层。

5.2 安全使用社交媒体服务

鉴于使用社交媒体可能带来的潜在风险，各决策局 / 部门在订阅社交媒体服务前，应进行风险评估，以评估相关的风险和估计潜在影响。当各决策局 / 部门决定订阅社交媒体服务时，应采取安全措施和控制措施，以防止和减低已被确认的风险至可接受的水平。

5.2.1 用户

帐户

- 每次使用社交媒体帐户后退出帐户，尤其是使用公共计算机或流动装置时。
- 在社交媒体平台上注册的电邮帐户，尽量与个人通讯的电邮帐户分开。
- 若非官方的参与，切勿在任何社交网站上使用政府电邮帐户进行注册。
- 避免自动登入社交媒体应用程式。

- 避免使用「社交媒体帐户登入」功能登入第三方应用程式及网站。
- 监察链接社交媒体帐户的电子邮件内的可疑链接，并确保帐户不受影响。
- 应确认社交媒体平台会否将用户的个人资料分享予第三方、所分享的资料种类和分享的目的。

密码

- 遵守部门的密码政策，使用严谨密码。例如，使用至少八个字符组成，包括大小写不一的字母、数字及特殊字符。
- 建议开启多重认证或至少双重认证来增加额外的保护层。
- 每个社交媒体帐户使用独立的登入名称和密码。
- 定期更改社交媒体帐户密码。
- 在使用公共计算机时（如在图书馆或网吧），使用一次性密码登入社交媒体帐户。
- 如果怀疑自己的帐户有任何问题，立即更改密码。
- 不要与他人分享社交媒体帐户的密码或验证码。
- 不要使用容易被猜到的密码，也不要在各种社交网站上使用相同密码。

安全设定

- 定期检查当前的安全和私隐设定、用户存取和发布的权限。
- 定期检查登入对话并立即终止未能识别的对话。
- 按照供货商建议的任何安全设定，并根据需要配置私隐设定。
- 开启双重认证，以加强帐户的安全性。
- 在适当情况下开启端对端加密。
- 开启获取未能识别的登入警示（如未能识别的计算机或流动装置）。
- 开启流动装置的密码锁，并设定不超过数分钟的空闲时间。
- 定期检查最近使用或允许的应用程序设定，删除不再需要的应用程序。
- 定期检查过往发布的帖文，删除不再想分享的帖文。
- 审视最新私隐政策，并评估所涉及的个人资料私隐风险。

发布

- 在发布看起来可能是微不足道的个人资料前，请三思而后行。虽然一些资料看起来可能无伤大雅（如宠物名字），但实际上它可能为恶意者提供丰富资料。恶意者可透过收集这些信息，冒充用户以获取敏感资料。
- 发布帖子前，应考虑信息的公开程度（如只限朋友或是任何人）。
- 不要过度分享个人资料，如住址、出生日期、电话号码以及有关日程或惯常出行路线的资料。
- 不要在社交媒体平台上发布敏感资料或非法内容。
- 在核实网站有效性和安全性之前，不应透过互联网发送敏感资料。
- 不要分享或转发社交媒体平台的帖子或电子邮件到另一个社交媒体平台上，因为它们可能存有关于帐户的敏感资料。
- 不要使用个人社交媒体帐户发布内部资料，如员工号码、组织架构、业务

合约、业务计划或日程，以及客户或商业伙伴的资料。
- 应尊重别人私隐权，未取得当事人同意前不要分享其个人资料。

网络和端点
- 经常使用安全的网络（包括安全的 Wi-Fi 网络）连接到社交媒体平台（不论是网站或流动应用程式），以保护登入帐户。
- 在社交媒体应用程序上安装最新的安全修补程序。
- 在端点上安装抗恶意软件软件及最新的安全修补程序，启动实时侦测，并保持抗恶意软件软件标识符及定义是最新的。
- 不应在公共场所使用不可信任的装置访问社交媒体帐户。

意识
- 留意使用操纵或欺骗手段试图获取资料的社交工程攻击。
- 对不熟悉的人发送的资料应时刻警惕，应避免点击来自不认识的人或源头不明的连结。
- 对陌生人持怀疑态度，必要时封锁垃圾邮件发送者。
- 收到别人的邀请时应时刻警惕，透过查看其资料和评价来核实。
- 要注意纠缠不清的应用程式和社交媒体 / 电邮帐户。
- 对社交媒体平台的安全警报和新闻应时刻警惕。
- 对社交媒体网站上发布的连结要谨慎。恶意网站或连结看似和正常网站相同，而只是在拼写上有些微变化。
- 遵守《使用电子邮件实务指南》第 3 节关于在公务中使用电子邮件的良好作业模式。
  （https://itginfo.ccgo.hksarg/content/imx/email_practice_guide.asp）
- 不应相信网上的内容，尤其是陌生人的资料。人们可能会发布虚假或误导性资料，甚至其个人身份。
- 不应点击陌生人或不明来源的连结。然而，即使访问认识的人的页面，点击链接或照片时也一定要小心，因为链接、应用程式或其他文件格式可能包含恶意代码。
- 不应下载和安装不熟悉的应用程式或插件。
- 不应相信在网上刚认识的人，就像不要相信在街上遇到的陌生人一样。
- 不应在任何已有超级用户权限的 Android 或已越狱的 iOS 装置上执行社交媒体流动应用程式。

5.2.2 管理员

管理员须遵守第 5.2.1 节对于一般用户的安全措施和控制措施，以及管理员执行指定工作职责的额外指定安全措施和控制措施。

以下是管理员的安全措施和控制措施：

一般管理

- 各决策局 / 部门应制订社交媒体帐户管理员的职务和职责，包括使用、管理和操作。
- 各决策局 / 部门应委任最少两名人员为管理员，并应充分利用职务分工。
- 制定使用社交媒体政策，确保敏感资料和保密资料不被披露。这些政策应清楚订明指引，使参与者了解哪些资料可分享，可与谁分享资料，以及甚么资料不能分享。
- 制定违反政策的纪律处分程序。

帐户

- 尽量使用不同帐户管理官方社交媒体专页和个人社交媒体帐户。如果社交媒体平台要求使用真实和个人帐户作为管理员或编者，建议决策局 / 部门采用合适的管理工具（例如 Facebook 企业管理平台）以便更好地跨专页管理帐户。
- 停用或关闭不再使用或无效的社交媒体帐户及网页。
- 遵守法律法规和知识产权。

密码

- 每个官方社交媒体帐户使用独立密码。
- 在可行的情况下，强制执行多重认证。
- 官方社交媒体帐户的密码只能由该社交媒体帐户的管理员保管，不得与他人共享。
- 当指定人员离开政府岗位时，立即更新密码和复原资料。

发布

- 为在所有官方社交媒体网页上发布帖子建立一个审批流程。
- 制定和编制发布内容的要求和程序。
- 制定举报任何滥用或安全问题的内部渠道和程序。
- 定期监察社交媒体帐户的帖子。所有帖子应由管理员审查和批准，以确保遵行社交媒体政策。
- 透过仲裁删除非法内容和过滤垃圾评论。可以通过建立一个机制去识别和举报网络攻击的来源（例如仿冒诈骗）和科技罪案（例如网上骗案），以补充仲裁程序。

网络和端点

- 在互联网网关安装防火墙和其他网络安全装置，并确保人员的计算机已安装最新安全修补程序，及配备最新定义档案的抗恶意软件软件，以提供额外防御层防止网络攻击和仿冒诈骗。

意识

- 对社交媒体平台的安全警报和新闻应时刻警惕，并将相关信息告知相关人员。
- 定期向人员提供有关政府信息安全政策的安全培训，并加强他们对于相关威胁的信息安全意识。

对于使用官方社交媒体帐户的政府指定人员，在官方网页上发帖的安全考虑包括但不限于：

- 遵守政府的行为守则，这些守则也适用于网络互动。
- 遵守社交媒体平台的行为守则、政策和服务条款。
- 在社交媒体平台发布前，对潜在的声誉风险进行风险监察。
- 不要发布任何保密资料，包括敏感的员工资料及足以辨识身分的资料。
- 不要在平台上传播虚假新闻、信息、照片和影片。
- 不要发布任何产品／服务广告或非公开的政府或决策局／部门的活动。
- 不要发布任何违反私隐条例、版权或知识产权的信息、照片或影片。
- 不要发布任何不当或未经授权的使用商标、销售或促销伪冒商品和诽谤信息。
- 不要传播垃圾邮件、恶作剧电子邮件、仿冒诈骗和网上诈骗。
- 不要发布可能影响政府人员中立性的信息。
- 不要发布任何涉及宣传非法活动、恶意网络攻击或销售受管制的商品和服务（如毒品、在线赌博）的内容。

为更有效地在社交媒体平台上保障个人资料，决策局／部门应遵守个人资料私隐专员公署制订的以下指引：

- 保障个人资料私隐－使用社交媒体及即时通讯软件的指引 (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/social_media_guidance.pdf)

- 机构智用社交网络 尊重个人资料私隐 (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/sn_organisational_c.pdf)

- 在网络世界保障私隐 精明使用社交网 (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/SN2015_c.pdf)

5.3 社交媒体帐户外泄及安全事故处理

社交媒体帐户的可疑活动包括自动按赞、不明状态更新和接收不明位置访问帐户的通知。安全事故处理程序须进行检讨和作出必要的修改以处理可疑征状。如果发生信息安全事故，用户应按照安全事故处理程序及时上报。

决策局 / 部门应特别考虑以下处理社交媒体帐户外泄的良好作业模式：

- 暂时停用社交媒体帐户。
- 收集和审查所有恶意活动的工件及记录，以进行调查及可能作为法律依据。
- 立即更改帐户密码。
- 更改相关电子邮件的密码。
- 核实帐户以备用电邮地址或短讯服务接收恢复密码验证码的选项。
- 核实帐户和相关电子邮件的自动转发选项。
- 从社交媒体帐户的网页删除任何可疑的应用程序。
- 必要时向政府信息安全事故应急办事处报告，例如涉及保密资料外泄。

附件 A - 常见社交媒体平台的安全提示

不同社交媒体平台的安全和私隐控制措施可能会有所不同，并随时间而改变。社交媒体帐户管理员应定期审视相关措施，以确保现行的安全控制措施符合各决策局 / 部门的要求。决策局 / 部门在制订安全政策时应参考官方建议。

1. Facebook

类别	网址
安全中心	https://zh-cn.facebook.com/safety
基本隐私设定和工具	https://www.facebook.com/help/325807937506242/

2. Twitter

类别	网址
如何保护和解除保护你的 Twitter? (只有英文版)	https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public

3. Instagram

类别	网址
隐私设定和信息	https://help.instagram.com/196883487377501

4. YouTube

类别	网址
隐私权与安全中心	https://support.google.com/youtube/topic/2803240?hl=zh-Hant&ref_topic=6151248

5. WhatsApp

类别	网址
隐私和安全的常见问题	https://faq.whatsapp.com/general/security-and-privacy/?lang=zh_cn

6. 微信

类别	网址
帐号安全	https://weixin110.qq.com/security/readtemplate?t=security_center_website/index

7. Telegram

说明	网址
安全 (只有英文版)	https://telegram.org/faq#security

8. LinkedIn

说明	网址
管理帐号和隐私设置	https://www.linkedin.com/help/linkedin/answer/66?lang=zh-hans

9. Snapchat

说明	网址
隐私设置 (只有英文版)	https://support.snapchat.com/en-GB/a/privacy-settings2

附件 B - 正确使用互联网

B.1 引言

互联网访问使政府人员能够有效地传播信息、与公众沟通和进行业务。虽然互联网访问可以提高生产力和改善沟通，但是，如用户不慎使用互联网，它亦存在风险。本附件列举一些与互联网访问有关的常见风险，并提供用户和网络管理员应采取的安全措施。

B.2 与使用互联网访问有关的风险

政府面临的风险和威胁是：

a) 丢失或外泄敏感资料（包括保密资料和个人资料）

互联网访问提供一个方便传输资料的方式。如果没有适当资料保护的控制措施，敏感资料可能会遭外泄或被意外地披露给未经授权的人士。例如，人员可能故意将敏感资料发送或发布到互联网。

b) 盗取凭证 – 导致未经授权的访问

由于广泛的互联网网站或服务，有些假网站会试图欺骗用户输入其凭证。如果用户没有意识到这些是虚假网站并输入他们的凭证，他们的资料可能会被用于未经授权访问系统。

c) 恶意内容或恶意软件

由于互联网访问服务容许用户通过其部门工作站或装置访问各种网站和服务，有可能使这些工作站或装置暴露于恶意内容或恶意软件，从而感染同一网络的其他工作站或装置。

d) 社交工程攻击（如仿冒诈骗）

黑客或攻击者可能收集用户在互联网，特别是社交媒体上发布的资料，并进行针对性的攻击，例如假装高级管理人员发送假电子邮件，以获未经授权访问信息系统。

e) 网络跟踪

网络跟踪者可能根据在互联网上收集的资料对用户进行跟踪。有一些个案是用户在社交媒体平台上发布个人资料（例如放假期间的照片）后被盗窃。

f) 涉及非法活动

通过政府互联网服务进行非法活动（如明知地访问恶意网站而招致分布式拒绝服务攻击、黑客攻击、下载 / 托管盗版软件、感染勒索软件以获取金钱等）或影响政府信息系统时，会影响政府声誉或形象。这些事件会令政府声誉受损，而涉事人员可能会受到处分。

B.3 用户指导原则

为了更好地保护政府资产，各决策局 / 部门应定期向用户提供有关正确使用互联网的培训和提醒。

所有政府人员在使用政府提供的互联网服务时应了解其义务和责任，并遵从政府所提供的互联网服务的使用条款。《使用互联网服务的指导原则》可查阅如下：

https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices/Guide_use_of_Internet.htm

B.4 管理员的指导原则

各决策局 / 部门应安排定期和特别培训，重点是正确使用互联网服务，以提高人员的信息安全意识。除了教育用户的责任外，各决策局 / 部门的管理员在向用户提供互联网服务时，应尽职尽责保护政府网络。

管理员**须**：

a) 遵守《互联网网关安全实务指南》的良好作业模式 (https://itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/Current/core/IGS_SC.pdf)
b) 更新部门的信息技术安全政策和指南以把已更新的指导原则适当地纳入。
c) 通知新用户，并定期通知所有用户遵守互联网访问服务的服务条款，确保人员知情和接受服务条款，并提醒他们每一位用户都要对其在信息系统上所有活动及其后果负责。
d) 对用户活动进行系统记录
    i. 保存分配给其管理的工作站或装置的固定互联网规约地址的记录。
    ii. 保存所有网络装置的动态互联网规约地址分配列表（或通常称为动态主机配置协议服务器列表），因为互联网访问服务系统在识别各决策局 / 部门的用户工作站内没有这些资料。
    iii. 各决策局 / 部门须保存本地代理服务器的活动记录。鼓励各决策局 / 部门在连接互联网访问服务的本地代理服务器中开启 X-Forwarded-For（XFF）头字段，以标明用户工作站的互联网规约地址。
    iv. 记录和审视用户的活动，以达到以下目的：
        - 系统诊断和故障排除；
        - 能力规划和服务改进；
        - 经调查确定互联网规约地址；以及
        - 应各决策局 / 部门的要求或根据法律规定提供信息。
e) 保留至少六个月互联网访问记录。
f) 在网关部署网络层面的保护（如互联网访问服务通讯闸、互联网通讯闸）。
g) 在互联网访问的工作站和装置上部署抗恶意软件软件。
h) 对所有系统、工作站和装置安装安全修补程序。
i) 避免通过文件传输通讯规约等未加密规约进行数据传输。