數字政策辦公室

資訊保安

社交媒體保安

實務指引

第 1.2 版

2024 年 7 月

版權公告

修改記錄

修改次數	修改詳情	經修改頁數	版本編號	日期
1	增加關於個人資料保護的保安風險及措施建議；更新常見社交媒體平台的保安提示的網址。	8; 14; 16-19; 21-22	1.1	2021 年 6 月
2	將「政府資訊科技總監辦公室」更改為「數字政策辦公室」		1.2	2024 年 7 月

目錄

1. 簡介 1

1.1 目的 1
1.2 參考標準 1
1.3 定義及慣用詞 2
1.4 聯絡方法 2

2. 資訊保安管理 3

3. 社交媒體概覽 5

3.1 社交媒體介紹 5
3.2 常見社交媒體類別 5

4. 社交媒體保安風險與威脅 7

4.1 對社交媒體參與者的威脅 7
4.2 社交媒體平台和服務的威脅 8
4.3 對政府和資料的威脅 11

5. 社交媒體保安措施和控制 12

5.1 社交媒體使用生命週期 12
5.2 安全使用社交媒體服務 14
5.3 泄露社交媒體帳戶及保安事故處理 19

附件 A - 常見社交媒體平台的保安提示 20

附件 B - 正確使用互聯網 22

1. 簡介

不論是個人或商業用途，社交媒體都越來越受歡迎。正確使用社交媒體可以改善公眾形象，成為有效的宣傳工具。另一方面，使用社交媒體也存在不少保安風險。各決策局／部門在使用社交媒體作為與公眾溝通的官方工具時，應小心謹慎，評估風險，並採取適當的保護措施。

1.1 目的

本實務指引旨為各決策局／部門提供通用的保安考慮和良好作業模式，以管理和使用社交媒體。本文件第 4 節描述使用及管理社交媒體的良好作業模式。社交媒體是一種基於互聯網的應用。故此，用戶需要正確使用互聯網，以保障資訊科技環境的保安。有關互聯網保安的考慮因素，請參閱**附件 B**。

本文件應按需要與其他保安文件如《基準資訊科技保安政策》[S17]、《資訊科技保安指引》[G3] 及相關程序和指引一同使用。

1.2 參考標準

以下參考文件為本文件在應用上不可或缺的參考：

- 香港特別行政區政府《基準資訊科技保安政策》[S17]
- 香港特別行政區政府《資訊科技保安指引》[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 定義及慣用詞

本文件將會採用《基準資訊科技保安政策》和《資訊科技保安指引》內所使用，以及以下的定義及慣用詞。

縮寫及術語	
不適用	不適用

1.4 聯絡方法

本文件由數字政策辦公室編製及備存。如有任何意見或建議，請寄往：

電郵： it_security@digitalpolicy.gov.hk

Lotus Notes 電郵： IT Security Team/DPO/HKSARG@DPO

CMMP 電郵： IT Security Team/DPO

2. 資訊保安管理

資訊保安是關於保安控制和措施的規劃、實施和持續提升，以保護資訊資產的機密性、完整性和可用性，適用於資訊的存儲、處理或傳輸過程及其相關資訊系統中。資訊保安管理是一套有關規劃、組織、指導、控制的原則和應用這些原則的法則，來迅速有效地管理實體、財務、人力資源和資訊資源，以及確保資訊資產和資訊系統的安全。

資訊保安管理涉及一系列需要持續監測和控制的活動。這些活動包括但不限於以下的範疇：

- 保安管理框架與組織；
- 管治、風險管理和遵行要求；
- 保安操作；
- 保安事件和事故管理；
- 保安意識培訓和能力建立；和
- 態勢感知和資訊共享。

保安管理框架與組織

決策局／部門須根據業務需要和政府保安要求，制定和實施部門資訊保安政策、標準、指引和程序。

決策局／部門亦須界定資訊保安的組織結構，並為有關各方就保安責任提供清晰的定義和適當的分配。

管治、風險管理和遵行要求

決策局／部門須採用風險為本的方法，以一致及有效的方式識別資訊系統的保安風險、訂定應對風險的緩急次序和應對有關風險。

決策局／部門須定期和在必要時對資訊系統和生產應用系統進行保安風險評估，以識別與保安漏洞相關的風險和後果，並為建立具成本效益的保安計劃和實施適當的保安保護和保障措施提供依據。

決策局／部門亦須定期對資訊系統進行保安審計，以確保當前的保安措施符合部門資訊保安政策、標準和其他合約或法律上的要求。

保安操作

為保護資訊資產和資訊系統，決策局／部門應根據業務需要實施全面的保安措施，涵蓋業務上不同的技術領域，並在日常操作中採取「預防、偵測、應變和復原」原則。

- 預防措施避免或阻止不良事件的發生；
- 偵測措施識別不良事件的發生；
- 應變措施是指在發生不良事件或事故時，採取協調行動來遏制損害；和
- 復原措施是將資訊系統的機密性、完整性和可用性恢復到預期狀態。

保安事件和事故管理

在現實環境中，由於存在不可預見並致服務中斷的事件，故此保安事故仍可能會發生。若保安事件危及業務的連續性或引起數據保安風險，決策局／部門須啟動其常規保安事故管理計劃，以實時識別、管理、記錄和分析保安威脅、攻擊或事故。決策局／部門亦應準備與有關各方適當地溝通，透過分享對有關保安風險的應變以消除不信任或不必要的猜測。當制定保安事故管理計劃時，決策局／部門應規劃和準備適當的資源，並製定相關程序，以配合必要的跟進調查。

保安意識培訓和能力建立

因為資訊保安每個人都有責任，所以決策局／部門應不斷提升機構內資訊保安意識，透過培訓及教育，確保有關各方了解保安風險，遵守保安規定和要求，並採取資訊保安的良好作業模式。

態勢感知和資訊共享

因應網路威脅形勢不斷變化，決策局／部門亦應不斷關注由保安行業和政府電腦保安事故協調中心發布的現時保安漏洞訊息、威脅警報和重要通知。應將即將或已經發生具威脅的保安警報傳達及分享給決策局／部門內的負責同事，以便採取及時的應對措施來緩解風險。

決策局／部門可以使用威脅情報平台來接收和分享有關保安問題、漏洞和網路威脅情報的資訊。

3. 社交媒體概述

3.1 社交媒體介紹

社交媒體是指參與者在互動平台上進行互相交流。近年來，社交媒體被普及使用。起初，Facebook、Instagram 和 YouTube 等社交媒體平台的用戶建立具有共同興趣的朋友網絡。現在，它不僅用於個人分享，還用作為商業或政府的溝通渠道，與公眾或目標觀眾互動和合作，以徵求意見和看法。然而，在網絡保安方面，這可帶來一定的相關風險。

在政府內部，參與社交媒體的決定應該由運作需求主導，並得到管理層的支持，亦應考慮到範圍、威脅、技術能力和潛在利益。為了抵禦社交媒體迅速發展的威脅，應制定風險管理方案，以評估風險並將其降低到可接受的水平。在保護參與者、平台和服務以及政府人員和資料方面，應考慮採取縱深防禦的緩解措施[1]。

3.2 常見社交媒體類別

隨著社交媒體的日益普及和強大，用戶享受社交媒體平台所帶來的不同網絡的好處。以下是用戶廣泛使用的常見社交媒體類別。

社交網絡

- 社交網絡使用戶可以與其他用戶和品牌線上聯繫，並鼓勵知識共享，實現人與人之間的互動。

媒體分享平台

- 媒體分享平台使用戶可以分享各種視覺內容，如影片、圖像、資訊圖和插圖。與社交網絡不同的是，這平台着重於分享視覺內容，並經過優化以幫助創作者上載其視覺內容並與其他觀眾互動。

[1]縱深防禦是透過利用分層保護和控制措施的方法，以保護資訊系統和資料。

論壇和社交社區

- 論壇和社交社區是指人們可以通過發佈資訊的形式進行對話，以獲得集體知識的線上討論網站。用戶可以匿名，也可以在論壇上註冊一個用戶名稱，然後再發佈資訊。

博客網絡

- 博客網絡使用戶和公司可以在線上發佈內容，幫助提高讓觀看者發現發佈內容的可見性。這種類型的社交媒體通常用於建立參與度，讓人們熟悉博客。

4. 社交媒體保安風險與威脅

決策局／部門應制定風險管理方案，以瞭解威脅並評估社交媒體參與者、平台和服務，以及決策局／部門（即訂戶）和所涉及的資料的相關風險。

- 參與者：一般公眾用戶，如參與社交媒體平台的公眾。
- 社交媒體平台和服務：讓政府和公眾互相溝通、協作、互動和分享資訊的網上媒體平台。
- 決策局／部門：商業或公共服務提供者的社交媒體服務的訂戶。

4.1 對社交媒體參與者的威脅

社交媒體平台存在與公眾參與者（例如在論壇發佈訊息的市民）相關的保安威脅。保安威脅包括私隱威脅、丟失登入憑證、惡意內容和程式碼、社交工程攻擊等。

私隱威脅

社交媒體，如論壇和博客，容許參與者向公眾發佈資訊或內容。這些交流形式可能因放置過多個人資料而帶來私隱問題，平台或容許根據個人行為而製作個人檔案，並作出對用戶不利的決定。如果參與者在社交媒體平台上發佈過多個人資料，可能會對參與者造成潛在的不利局面。這此資料會留下永久的數碼足跡，難以從網絡世界中移除，而且或會被濫用於身份盜用。

被盜或丟失登入憑證

如果密碼揀選不當或保護不當，惡意者會設法盜取密碼。如在未經授權下登入帳戶，惡意者可能會發佈假冒訊息或利用帳戶傳播惡意軟件。

惡意內容、程式碼和仿冒詐騙連結

由於用戶數量和發佈個人資訊的數量眾多，社交媒體已成為其中一個攻擊向量而此攻擊亦逐漸普遍。攻擊者可能會利用這渠道傳播惡意內容、程式碼或仿冒詐騙連結。如果社交媒體網站存在保安漏洞，攻擊者能編寫看似正常的應用程式，使電腦在用戶不知情的情況下受到感染。

社交工程攻擊

社交媒體建立具有一定人際信任度的網絡社區。惡意者可冒充用戶信任的人，並說服他們披露敏感資料。此外，在使用一些社交工程技能時，攻擊如病毒、特洛依木馬或謠言等能容易地和迅速地傳播。

4.2 對社交媒體平台和服務的威脅

對於社交媒體平台和服務存在的威脅，如服務供應商提供的論壇、博客和即時通訊等。就威脅的影響而言，平台的正常運行可能會受到干擾、服務可能會被中斷，以及資料可能會被未經授權的存取和披露。

以下是對於社交媒體平台和服務的常見威脅：

緩衝區滿溢

緩衝區滿溢是一種廣為人知的軟件保安漏洞。在經典的緩衝區滿溢漏洞，攻擊者將數據發送到程式，而程式將其存儲在一個容量過小的堆疊緩衝區。結果是呼叫堆疊的資料被蓋寫，當中包括函數的返回指標。由於數據設置返回指標的價值，所以當函數返回時，會把控制權轉移到攻擊者數據中包含的惡意程式碼。

遠程代碼執行漏洞

攻擊者利用漏洞執行惡意程式碼，並利用用戶的權限完全控制受影響的平台／系統。在接達平台／系統後，攻擊者會試圖提升其權限。

濫發郵件

濫發郵件是針對社交媒體網站傳播垃圾郵件的常見攻擊方式。它濫用電子訊息系統，大量發送未經請求的訊息。論壇濫發郵件是指那些辱罵、行銷噱頭、或是無用的資訊。在論壇沒有管理的情況下，濫發郵件可以頻繁地發生。它可能在短短幾個小時，甚至幾分鐘內發生，甚至可能由於資訊氾濫而導致論壇伺服器停止服務。這將消耗資訊系統的資源，並對其他正常服務的服務水平產生負面影響。更重要的是，參與者可能會發現社交媒體平台上充斥著無用的資訊，並且對參與進一步的討論失去興趣。

網上應用程式攻擊

網上應用程式是使用動態網頁為參與者提供額外的功能。然而，這些額外的功能可能意味著有更多攻擊網上應用程式的機會。這使社交媒體網站為攻擊者開啓了可利用的廣泛保安漏洞。攻擊者可通過鍵次登入器以捕捉用戶的鍵擊，包括帳戶用戶名稱和密碼。若個人社交媒體帳戶被劫持或會令人感到煩惱、尷尬甚至付出

代價，而當政府官方帳戶被劫持時，可能會帶來更嚴重的影響。非官方帖子或訊息可能被公眾視為官方訊息，或可被用於傳播惡意軟件，使用戶在不知情下點選連結或下載不需要的應用程式。

以下是一些常見的網上應用攻擊的例子：

- 無效身份認證
  與身份認證和對話管理相關的應用功能經常被錯誤地推行，允許攻擊者破解密碼、金鑰或對話權標，或利用其他應用程式的缺陷，暫時或永久地冒充其他用戶的身份。

- 無效存取控制
  存取控制是指控制資訊或存取功能的系統。無效存取控制允許攻擊者繞過授權，並扮演管理員等特權用戶以同等特權執行任務，例如一個網上應用程式允許用戶在沒有任何其他驗證的情況下，只需更改統一網址的一部分，就可更改他們所登錄的帳戶。

- 敏感資料泄露
  許多網上應用程式和應用程式界面沒有適當地保護敏感資料，如金融、醫療和個人可識別訊息。攻擊者可能會竊取或修改受較弱保護的資料，以進行信用卡欺詐、身份盜竊或其他犯罪行為。敏感資料可能會在沒有額外保護的情況下被泄露，例如資料在沒加密的儲存或傳輸過程中，因此在使用瀏覽器時需要特別的預防措施。

- 跨網站指令碼
  跨網站指令碼是一種網上應用程式攻擊，誘使終端用戶的網頁瀏覽器執行惡意程式碼。惡意程式碼可能會竊取終端用戶的個人資料，從而攻擊者可冒充終端用戶，操縱終端用戶的電腦，在受害者不知情的情況下，發起攻擊。

- 跨網站請求偽造
  跨網站請求偽造是一種網上應用程式攻擊，導致終端用戶的網頁瀏覽器在用戶不知情的情況下，執行攻擊者選擇行動。通過在網頁中嵌入惡意連結或通過電子郵件或聊天發送連結，攻擊者可能導致網上應用程式的用戶執行不必要的行動。更具體地說，攻擊者導致用戶的瀏覽器在用戶或網站不知情的情況下，向已通過驗證的網站發出請求。這些行動可能損害終端用戶的資料和操作，甚至令到整個伺服器或網絡受損。

- 注入攻擊
  社交媒體使用的技術使其容易受到注入攻擊，例如可擴充標記語言和結構化查詢語言的注入。此外，社交媒體應用程式通常依賴於客戶端代碼，因此它們嚴重依賴於攻擊者可繞過的客戶端輸入驗證。

不恰當或具侵犯性的內容

參與者可能會在社交網站上發佈或上傳不恰當或具侵犯性的內容。內容可能包括未經版權授權的材料、社會普遍未能接受的道德標準或範圍、有關網絡攻擊或藥物使用等。發佈這些內容可能影響政府形象。另一個顧慮是持有這些不合法內容的最終責任。

未經授權的內容變更或服務中斷

在線破壞行為涉及對在線資產的損害或破壞，可能影響政府形象和聲譽。行為範圍從網址篡改到服務中斷。

仿冒詐騙

仿冒詐騙是一種針對特定用戶或用戶群組的有效攻擊，欺騙用戶執行會發起攻擊行動的行為，例如打開文件或點擊連結。仿冒詐騙者依靠了解目標的個人資料，例如興趣、旅行計劃、社交圈子等。大多數時候，個人資料只是通過在社交媒體上來收集。仿冒詐騙者利用社交媒體作為另一種方式發送詐騙訊息，因為社交媒體平台繞過傳統電子郵件保安控制。仿冒詐騙者在社交媒體上發佈的連結可能看似正常網站，而在拼寫上有些微變化，或者使用不同網域欺騙用戶。

可用性和效能

由於硬體或軟件問題，可能會出現服務中斷的情況，或者系統容量達到極限，導致效能下降。如果發生災難，服務可能完全無法使用，業務連續性將受到影響。另外，服務供應者（或其承辦商）可能會倒閉，或在發生糾紛時挾持資料。服務供應者（及其承辦商）的可信度、可靠性和能力對確保社交媒體服務的持續是非常重要。

4.3 對決策局／部門和資料的威脅

在網站上提供社交媒體平台的服務，將具有容易接觸大量參與者的優勢。因此，公共社交媒體平台往往是以社交媒體為目的而部署。不論在內部基礎設施上部署，或是外判至服務供應者，這些都會令政府人員和資料受到威脅。

以下是特別針對政府人員和資料的常見威脅：

披露內部／保密資料

敏感或保密資料可能有意或無意地被披露，使政府聲譽受損或陷入尷尬。

保留和銷毀資料

各種原因可能導致決策局／部門與服務供應商終止協作，例如技術轉變、普及程度、合約期屆滿及未能續約。在這些情況下，決策局／部門無法從社交媒體平台取回所有資料可能會導致出現數據遺失風險。另一方面，服務供應者可能沒有依照適當程序棄置政府資料。

資料不正當使用

社交媒體供應者可能沒有充分保障用戶或參與者的私隱，以確保資料不會被用作其他用途及不可向第三方披露。服務供應商可能會收集參與者的登記資料作市場推廣用途，這在一定程度上，可能會對參與者造成滋擾。

對服務和資料的有限控制

根據社交媒體服務的訂購協議，資料通常在雲端環境下儲存和處理。在該環境下，對平台甚至政府資料的控制可能受到限制。例如，你可能無法要求對整個硬碟進行影像備份，因為它包含其他訂購者的資料。

缺乏意識

缺乏意識可導致不同程度的保安漏洞。社交工程攻擊可能針對政府人員，其中負責人員如社交媒體管理員可能被欺騙而泄露身份資料。此外，員工可能會在社交媒體上發佈內部或機密資訊，影響政府形象。

假冒

假冒者往往在社交媒體上建立類似名人、商業機構或政府官員的帳戶。一些假冒他人的帳戶可能帶有欺騙意圖，給公眾傳達誤導性的訊息，以收集資訊或獲取財務利益。

5. 社交媒體保安措施和控制

5.1 社交媒體使用生命週期

5.1.1 提供社交媒體帳戶

各決策局／部門在考慮採用社交媒體時，應確定使用社交媒體的需求，以及社交媒體如何支持其業務。決策局／部門應制定使用社交媒體的政策，清楚訂明使用社交媒體服務的業務和保安要求。

5.1.1.1 建立社交媒體帳戶

根據使用情況和保安要求，各決策局／部門應制定適當的流程和程序以提供社交媒體帳戶。特別是，社交媒體帳戶的保安配置應按照政府的保安要求執行。有關強化保安的樣本配置，請參閱**附件 A**。

各決策局／部門應從高層管理人員中委任一名人員擔任社交媒體帳戶管理員主管，以及最少兩名人員擔任社交媒體帳戶管理員，為決策局／部門設立、接達和管理社交媒體帳戶。

管理員應建立、命名和組建代表政府或決策局／部門的社交媒體帳戶，並提供已得到管理員主管批准的資訊。這些資訊包括但不限於：

- 帳戶說明
- 業務資訊
- 聯繫方式（如電郵地址、網站）
- 地址
- 個人頭像的照片
- 一般資訊

5.1.1.2 社交媒體使用政策

為了規範管理員和用戶對社交媒體的使用，應制定適當使用社交媒體的保安政策。不同領域的社交媒體平台的常見保安和控制措施，包括但不限於：

- 一般管理
- 帳戶
- 密碼
- 保安設定
- 發佈
- 網絡和端點
- 意識

社交媒體服務的安全使用細節列於**第 5.2 節 – 安全使用社交媒體服務**。

5.1.1.3 使用社交媒體分析

社交媒體分析是在社交媒體平台收集和分析數據的過程。收集的資訊包括但不限於：

- 在社交媒體平台上分享的個人資料（如個人檔案資料、內容、使用情況以及第三方網站和應用程式）。
- 設備資訊（如設備識別號碼、屬性、操作、信號、網絡和連接以及小型文字檔案數據）
- 來自第三方夥伴和服務的資訊，包括廣告商和應用開發商（如帳戶資料、用戶設置和社交互動活動）。

決策局／部門應參考個人資料私隱專員公署出版有關網上行為追蹤的資料單張。

- 網上行為追蹤 (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/online_tracking_c.pdf)

社交媒體分析工具幫助用戶瞭解觀眾以及他們如何與社交媒體頁面中的帖子互動。它提供關於社交媒體帳戶的見解、指標和儀錶板，包括但不限於：

- 追隨者數量
- 追隨者的年齡層
- 帖子的觀眾參與度
- 追隨者訪問社交媒體頁面的時間和地點
- 社交媒體頁面上的帖子數量
- 內容曝光次數
- 讀取內容的人數
- 與內容進行互動的人數（如喜歡、分享、轉發、回覆或提及）

社交媒體帳戶管理員應該利用社交媒體分析技術，提供更好的服務，並與社會各界互動。

5.1.2 停用社交媒體帳戶

各決策局／部門應定期檢視社交媒體的使用情況。如社交媒體帳戶超過六個月沒有使用，管理員應考慮停用該帳戶。社交媒體帳戶管理員主管亦應將此事呈報至決策局／部門的高級管理層。

5.2 安全使用社交媒體服務

鑑於使用社交媒體可能帶來的潛在風險，各決策局／部門在訂閱社交媒體服務前，應進行風險評估，以評估相關的風險和估計潛在影響。當各決策局／部門決定訂閱社交媒體服務時，應採取保安措施和控制措施，以防止和減低已被確認的風險至可接受的水平。

5.2.1 用戶

帳戶

- 每次使用社交媒體帳戶後登出帳戶，尤其是使用公共電腦或流動裝置時。
- 在社交媒體平台上註冊的電郵帳戶，盡量與個人通訊的電郵帳戶分開。
- 若非官方的參與，切勿在任何社交網站上使用政府電郵帳戶進行註冊。
- 避免自動登入社交媒體應用程式。
- 避免使用「社交媒體帳戶登入」功能登入第三方應用程式及網站。

- 監察連結社交媒體帳戶的電子郵件內的可疑連結，並確保帳戶不受影響。
- 應確認社交媒體平台會否將用戶的個人資料分享予第三方、所分享的資料種類和分享的目的。

密碼

- 遵守部門的密碼政策，使用嚴謹密碼。例如，使用至少八個字元組成，包括大小寫不一的字母、數字及特殊字符。
- 建議開啓多重認證或至少雙重認證來增加額外的保護層。
- 每個社交媒體帳戶使用獨立的登入名稱和密碼。
- 定期更改社交媒體帳戶密碼。
- 在使用公共電腦時（如在圖書館或網吧），使用一次性密碼登入社交媒體帳戶。
- 如果懷疑自己的帳戶有任何問題，立即更改密碼。
- 不要與他人分享社交媒體帳戶的密碼或驗證碼。
- 不要使用容易被猜到的密碼，也不要在各種社交網站上使用相同密碼。

保安設定

- 定期檢查當前的保安和私隱設定、用戶存取和發佈的權限。
- 定期檢查登入對話並立即終止未能識別的對話。
- 按照供應商建議的任何保安設定，並根據需要配置私隱設定。
- 開啓雙重認證，以加強帳戶的安全性。
- 在適當情況下開啓端對端加密。
- 開啓獲取未能識別的登入警示（如未能識別的電腦或流動裝置）。
- 開啓流動裝置的密碼鎖，並設定不超過數分鐘的閒置時間。
- 定期檢查最近使用或允許的應用程式設定，刪除不再需要的應用程式。
- 定期檢查過往發佈的帖文，刪除不再想分享的帖文。
- 審視最新私隱政策，並評估所涉及的個人資料私隱風險。

發佈

- 在發佈看起來可能是微不足道的個人資料前，請三思而後行。雖然一些資料看起來可能無傷大雅（如寵物名字），但實際上它可能為惡意者提供豐富資料。惡意者可透過收集這些資訊，冒充用戶以獲取敏感資料。
- 發佈帖子前，應考慮資訊的公開程度（如只限朋友或是任何人）。
- 不要過度分享個人資料，如住址、出生日期、電話號碼以及有關日程或慣常出行路線的資料。
- 不要在社交媒體平台上發佈敏感資料或非法內容。
- 在核實網站有效性和保安性之前，不應透過互聯網發送敏感資料。
- 不要分享或轉發社交媒體平台的帖子或電子郵件到另一個社交媒體平台上，因為它們可能存有關於帳戶的敏感資料。
- 不要使用個人社交媒體帳戶發佈內部資料，如員工號碼、組織架構、業務

合約、業務計劃或日程，以及客戶或商業伙伴的資料。
- 應尊重別人私隱權，未取得當事人同意前不要分享其個人資料。

網絡和端點
- 經常使用安全的網絡（包括安全的 Wi-Fi 網絡）連接到社交媒體平台（不論是網站或流動應用程式），以保護登入帳戶。
- 在社交媒體應用程式上安裝最新的保安修補程式。
- 在端點上安裝抗惡意程式軟件及最新的保安修補程式，啓動即時偵測，並保持抗惡意程式軟件識別碼及定義是最新的。
- 不應在公共場所使用不可信任的裝置接達社交媒體帳戶。

意識
- 留意使用操縱或欺騙手段試圖獲取資料的社交工程攻擊。
- 對不熟悉的人發送的資料應時刻警惕，應避免點擊來自不認識的人或源頭不明的連結。
- 對陌生人持懷疑態度，必要時封鎖垃圾郵件發送者。
- 收到別人的邀請時應時刻警惕，透過查看其資料和評價來核實。
- 要注意糾纏不清的應用程式和社交媒體／電郵帳戶。
- 對社交媒體平台的保安警報和新聞應時刻警惕。
- 對社交媒體網站上發佈的連結要謹慎。惡意網站或連結看似和正常網站相同，而只是在拼寫上有些微變化。
- 遵守《使用電子郵件實務指引》第 3 節關於在公務中使用電子郵件的良好作業模式。
  （https://itginfo.ccgo.hksarg/content/imx/email_practice_guide.asp）
- 不應相信網上的內容，尤其是陌生人的資料。人們可能會發佈虛假或誤導性資料，甚至其個人身份。
- 不應點擊陌生人或不明來源的連結。然而，即使訪問認識的人的頁面，點選連結或照片時也一定要小心，因為連結、應用程式或其他檔案格式可能包含惡意程式碼。
- 不應下載和安裝不熟悉的應用程式或外掛程式。
- 不應相信在網上剛認識的人，就像不要相信在街上遇到的陌生人一樣。
- 不應在任何已有超級用戶權限的 Android 或已越獄的 iOS 裝置上執行社交媒體流動應用程式。

5.2.2 管理員

管理員須遵守第 5.2.1 節對於一般用戶的保安措施和控制措施，以及管理員執行指定工作職責的額外指定保安措施和控制措施。

以下是管理員的保安措施和控制措施：

一般管理

- 各決策局／部門應制訂社交媒體帳戶管理員的職務和職責，包括使用、管理和操作。
- 各決策局／部門應委任最少兩名人員為管理員，並應充分利用職務分工。
- 制定使用社交媒體政策，確保敏感資料和保密資料不被披露。這些政策應清楚訂明指引，使參與者瞭解哪些資料可分享，可與誰分享資料，以及甚麼資料不能分享。
- 制定違反政策的紀律處分程序。

帳戶

- 盡量使用不同帳戶管理官方社交媒體專頁和個人社交媒體帳戶。如果社交媒體平台要求使用真實和個人帳戶作為管理員或編者，建議決策局／部門採用合適的管理工具（例如 Facebook 企業管理平台）以便更好地跨專頁管理帳戶。
- 停用或關閉不再使用或無效的社交媒體帳戶及網頁。
- 遵守法律法規和知識產權。

密碼

- 每個官方社交媒體帳戶使用獨立密碼。
- 在可行的情況下，強制執行多重認證。
- 官方社交媒體帳戶的密碼只能由該社交媒體帳戶的管理員保管，不得與他人共用。
- 當指定人員離開政府崗位時，立即更新密碼和復原資料。

發佈

- 為在所有官方社交媒體網頁上發佈帖子建立一個審批流程。
- 制定和編制發佈內容的要求和程序。
- 制定舉報任何濫用或保安問題的內部渠道和程序。
- 定期監察社交媒體帳戶的帖子。所有帖子應由管理員審查和批准，以確保遵行社交媒體政策。
- 透過仲裁刪除非法內容和過濾垃圾評論。可以通過建立一個機制去識別和舉報網絡攻擊的來源（例如仿冒詐騙）和科技罪案（例如網上騙案），以

補充仲裁程序。

網絡和端點

- 在互聯網通訊閘安裝防火牆和其他網絡保安裝置，並確保人員的電腦已安裝最新保安修補程式，及配備最新定義檔案的抗惡意程式軟件，以提供額外防禦層防止網絡攻擊和仿冒詐騙。

意識

- 對社交媒體平台的保安警報和新聞應時刻警惕，並將相關資訊告知相關人員。
- 定期向人員提供有關政府資訊保安政策的保安培訓，並加強他們對於相關威脅的資訊保安意識。

對於使用官方社交媒體帳戶的政府指定人員，在官方網頁上發帖的保安考慮包括但不限於：

- 遵守政府的行為守則，這些守則也適用於網絡互動。
- 遵守社交媒體平台的行為守則、政策和服務條款。
- 在社交媒體平台發佈前，對潛在的聲譽風險進行風險監察。
- 不要發佈任何保密資料，包括敏感的員工資料及足以辨識身分的資料。
- 不要在平台上傳播虛假新聞、資訊、照片和影片。
- 不要發佈任何產品／服務廣告或非公開的政府或決策局／部門的活動。
- 不要發佈任何違反私隱條例、版權或知識產權的資訊、照片或影片。
- 不要發佈任何不當或未經授權的使用商標、銷售或促銷偽冒商品和誹謗資訊。
- 不要傳播垃圾郵件、惡作劇電子郵件、仿冒詐騙和網上詐騙。
- 不要發佈可能影響政府人員中立性的資訊。
- 不要發佈任何涉及宣傳非法活動、惡意網絡攻擊或銷售受管制的商品和服務（如毒品、線上賭博）的內容。

為更有效地在社交媒體平台上保障個人資料，決策局／部門應遵守個人資料私隱專員公署制訂的以下指引：

- 保障個人資料私隱－使用社交媒體及即時通訊軟件的指引 (https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/social_media_guidance.pdf)

- 機構智用社交網絡 尊重個人資料私隱 (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/sn_organisational_c.pdf)
- 在網絡世界保障私隱 精明使用社交網 (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/SN2015_c.pdf)

5.3 社交媒體帳戶外泄及保安事故處理

社交媒體帳戶的可疑活動包括自動按讚、不明狀態更新和接收不明位置接達帳戶的通知。保安事故處理程序須進行檢討和作出必要的修改以處理可疑徵狀。如果發生資訊保安事故，用戶應按照保安事故處理程序及時上報。

決策局／部門應特別考慮以下處理社交媒體帳戶外泄的良好作業模式：

- 暫時停用社交媒體帳戶。
- 收集和審查所有惡意活動的工件及記錄，以進行調查及可能作為法律依據。
- 立即更改帳戶密碼。
- 更改相關電子郵件的密碼。
- 核實帳戶以備用電郵地址或短訊服務接收恢復密碼驗證碼的選項。
- 核實帳戶和相關電子郵件的自動轉發選項。
- 從社交媒體帳戶的網頁刪除任何可疑的應用程式。
- 必要時向政府資訊保安事故應變辦事處報告，例如涉及保密資料外泄。

附件 A - 常見社交媒體平台的保安提示

不同社交媒體平台的保安和私隱控制措施可能會有所不同，並隨時間而改變。社交媒體帳戶管理員應定期審視相關措施，以確保現行的保安控制措施符合各決策局／部門的要求。決策局／部門在制訂保安政策時應參考官方建議。

1. Facebook

類別	網址
安全中心	https://zh-hk.facebook.com/safety
基本隱私設定和工具	https://www.facebook.com/help/325807937506242/

2. Twitter

類別	網址
如何保護和解除保護你的 Twitter？ (只有英文版)	https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public

3. Instagram

類別	網址
隱私設定和資訊	https://help.instagram.com/196883487377501

4. YouTube

類別	網址
隱私權與安全中心	https://support.google.com/youtube/topic/2803240?hl=zh-Hant&ref_topic=6151248

5. WhatsApp

類別	網址
隱私和安全的常見問題	https://faq.whatsapp.com/general/security-and-privacy/?lang=zh_tw

6. 微信

類別	網址
帳戶安全	https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?opcode=2&lang=zh_TW&plat=android&id=170417mEBB7N170417yaYFnA&Channel=helpcenter

7. Telegram

說明	網址
保安 (只有英文版)	https://telegram.org/faq#security

8. LinkedIn

說明	網址
管理帳戶和隱私設定	https://www.linkedin.com/help/linkedin/answer/66?lang=zh-hant

9. Snapchat

說明	網址
隱私設置 (只有英文版)	https://support.snapchat.com/en-GB/a/privacy-settings2

附件 B - 正確使用互聯網

B.1 引言

互聯網接達使政府人員能夠有效地傳播資訊、與公眾溝通和進行業務。雖然互聯網接達可以提高生產力和改善溝通，但是，如用戶不慎使用互聯網，它亦存在風險。本附件列舉一些與互聯網接達有關的常見風險，並提供用戶和網絡管理員應採取的保安措施。

B.2 與使用互聯網接達有關的風險

政府面臨的風險和威脅是：

a) 丟失或外泄敏感資料（包括保密資料和個人資料）

互聯網接達提供一個方便傳輸資料的方式。如果沒有適當資料保護的控制措施，敏感資料可能會遭外泄或被意外地披露給未經授權的人士。例如，人員可能故意將敏感資料發送或發佈到互聯網。

b) 盜取憑證 – 導致未經授權的接達

由於廣泛的互聯網網站或服務，有些假網站會試圖欺騙用戶輸入其憑證。如果用戶沒有意識到這些是虛假網站並輸入他們的憑證，他們的資料可能會被用於未經授權接達系統。

c) 惡意內容或惡意軟件

由於互聯網接達服務容許用戶通過其部門工作站或裝置接達各種網站和服務，有可能使這些工作站或裝置暴露於惡意內容或惡意軟件，從而感染同一網絡的其他工作站或裝置。

d) 社交工程攻擊（如仿冒詐騙）

駭客或攻擊者可能收集用戶在互聯網，特別是社交媒體上發佈的資料，並進行針對性的攻擊，例如假裝高級管理人員發送假電子郵件，以獲未經授權接達資訊系統。

e) 網絡跟蹤

網絡跟蹤者可能根據在互聯網上收集的資料對用戶進行跟蹤。有一些個案是用戶在社交媒體平台上發佈個人資料（例如放假期間的照片）後被盜竊。

f) 涉及非法活動

通過政府互聯網服務進行非法活動（如明知地訪問惡意網站而招致分布式拒絕服務攻擊、駭客攻擊、下載／託管盜版軟件、感染勒索軟件以獲取金錢等）或影響政府資訊系統時，會影響政府聲譽或形象。這些事件會令政府聲譽受損，而涉事人員可能會受到處分。

B.3 用戶指導原則

為了更好地保護政府資產，各決策局／部門應定期向用戶提供有關正確使用互聯網的培訓和提醒。

所有政府人員在使用政府提供的互聯網服務時應了解其義務和責任，並遵從政府所提供的互聯網服務的使用條款。《使用互聯網服務的指導原則》可查閱如下：

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

B.4 管理員的指導原則

各決策局／部門應安排定期和特別培訓，重點是正確使用互聯網服務，以提高人員的資訊保安意識。除了教育用戶的責任外，各決策局／部門的管理員在向用戶提供互聯網服務時，應盡職盡責保護政府網絡。

管理員**須**：

a) 遵守《互聯網通訊閘保安實務指引》的良好作業模式 (https://itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/Current/core/IGS_TC.pdf)
b) 更新部門的資訊科技保安政策和指引以把已更新的指導原則適當地納入。
c) 通知新用戶，並定期通知所有用戶遵守互聯網接達服務的服務條款，確保人員知情和接受服務條款，並提醒他們每一位用戶都要對其在資訊系統上所有活動及其後果負責。

d) 對用戶活動進行系統記錄

i. 保存分配給其管理的工作站或裝置的固定互聯網規約地址的記錄。

ii. 保存所有網絡裝置的動態互聯網規約地址分配清單（或通常稱為動態主機配置協議伺服器列表），因為互聯網接達服務系統在識別各決策局／部門的用戶工作站內沒有這些資料。

iii. 各決策局／部門須保存本地代理伺服器的活動記錄。鼓勵各決策局／部門在連接互聯網接達服務的本地代理伺服器中開啟 X-Forwarded-For（XFF）頭欄位，以標明用戶工作站的互聯網規約位址。

iv. 記錄和審視用戶的活動，以達到以下目的：

- 系統診斷和故障排除；
- 能力規劃和服務改進；
- 經調查確定互聯網規約地址；以及
- 應各決策局／部門的要求或根據法律規定提供資訊。

e) 保留至少六個月互聯網接達記錄。

f) 在通訊閘部署網絡層面的保護（如互聯網接達服務通訊閘、互聯網通訊閘）。

g) 在互聯網接達的工作站和裝置上部署抗惡意程式軟件。

h) 對所有系統、工作站和裝置安裝保安修補程式。

i) 避免通過檔案傳輸通訊規約等未加密規約進行數據傳輸。