數字政策辦公室

資訊保安

Wi-Fi 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	更新縮寫及術語	1	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

此文件旨在為不同的羣體服務，例如管理人員、系統擁有者、資訊科技保安管理員、區域網域網絡/系統管理員和資訊保安持份者，他們負責設置和管理政府內部的 Wi-Fi 網絡。

一些決策局／部門用戶可以使用具有多種通訊技術（包括 Wi-Fi）的流動裝置。有關採用流動裝置和相關管理的保安指引的詳細資訊，請參閱《流動保安實務指引》第 4 節。

1.1 目的

本文件的目的是為決策局／部門提供常見的保安注意事項和良好作業模式，以說明設計、管理和操作在政府裏的 Wi-Fi 網絡。本文件第 4 節介紹良好作業模式。

1.2 參考標準

以下參考文件對於本文件的應用是不可或缺：

- 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》，《資訊科技保安指引》和以下的術語及慣用詞。

縮寫及術語	
Wi-Fi	Wi-Fi 是基於 IEEE 802.11 系列的無線通訊技術
5G	5G 是指第五代的流動通訊技術，它是由國際電信聯盟為發展新一代流動科技而制定的。

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各項功能的領域：

- 保安管理框架和組織；
- 治理、風險管理和合規；
- 保安操作；
- 保安事件和事件管理；
- 意識培訓和能力建設；和
- 態勢感知和信息共用。

保安管理框架和組織

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架構，並為有關各方就保安責任提供清晰的定義和適當的分配。

治理、風險管理和合規

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。

意識培訓和能力建設

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的資訊保安意識，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

因應網絡威脅形勢不斷變化，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／部門可以利用威脅情報平台接收和分享保安事務、保安漏洞和網絡威脅情報的訊息。

3. Wi-Fi 保安概述

3.1 Wi-Fi 網絡簡介

Wi-Fi 是基於 IEEE 802.11 系列的無線通訊技術，通常用於各種資訊科技設備例如流動電話、可攜式電腦、全球定位系統設備以及物聯網裝置等，以存取局部區域網絡或互聯網。

Wi-Fi 使用高頻無線電波（而非有線），令資訊科技設備和裝置之間進行通訊。無線訊號的特點是有關訊號普遍在無線局部區域網絡所覆蓋的範圍內通過空氣傳輸，並且可以穿透實體邊界，如建築物牆壁和窗戶。因此，除非已採取保安措施防止透過無線傳遞不被「竊聽」，否則任何人都可以在實體邊界之外讀取此類訊號，帶來潛在的保安風險。連接到政府內部網絡的 Wi-Fi 須採取充分認證和傳遞加密措施，並輔之以適當的保安管理程序和良好作業模式。

3.2 典型的 Wi-Fi 網絡

此節簡要介紹典型的 Wi-Fi 網絡供參考。決策局／部門應根據業務需要和運作，決定其 Wi-Fi 網絡的配置。

典型的 Wi-Fi 網絡可以有四個主要部分：用戶端裝置、Wi-Fi 存取點（存取點）和網絡路由器/交換機、管理系統和互聯網通訊閘。用戶端裝置的例子包括筆記型電腦、平板電腦和智能手機。存取點提供用戶端裝置與網絡之間的無線連接。網絡路由器在後端連接存取點和管理系統。管理系統監察和控制 Wi-Fi 網絡上的活動。它通常包括無線入侵防禦系統、無線網絡管理系統、認證系統和抗惡意軟件程式系統。管理系統須要處理網絡和應用程式層面的保安威脅，例如未獲授權接達和惡意活動。互聯網通訊閘管理與互聯網服務供應商的連接。它還包括防火牆、入侵檢測或防禦系統以及將內部網絡連接到互聯網的路由器。

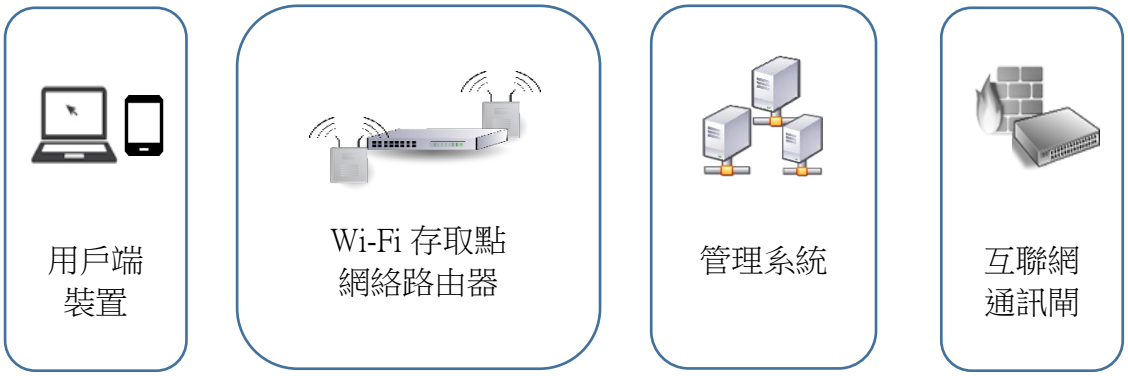

圖 1 典型 Wi-Fi 網絡的四個主要部分

4. Wi-Fi 網絡面對的威脅和漏洞

4.1 威脅和保安漏洞

現今無線連接藉其從大型機構到個人使用的電腦以及網絡等各個方面都被廣泛採用的優勢，令其得以起著重要的作用。然而，隨著無線網絡的可用性提高，也意味著遭受攻擊的危險也會相對增加，同時也為機構、資訊科技人員和資訊科技保安專業人員帶來更多挑戰。攻擊者可能試圖掌握關於網絡的資訊，以利用網絡保安漏洞。對網絡而言，這也是一項保安威脅。Wi-Fi 網絡的保安威脅描述如下。

Wi-Fi 存取點

- 破解有線等效保密規約/無線保護接達

  採用以前版本的保安協定（如有線等效保密規約或無線保護接達）作保護的無線網絡，因應現今的技術而言是不安全的。

- 存取點有不妥善的配置

  若存取點有寬鬆或不正確的設定，會容許未獲授權的裝置連線或使連接的通訊暴露在嗅探攻擊和重播攻擊中。

- 無線竊聽

  如果不妥善設定存取點而網絡通訊亦未經加密，敏感的通訊或系統事項將受到威脅。如果網絡通訊包含清晰的文字，惡意攻擊者便能夠使用竊聽工具取得敏感資料，如密碼或信用卡號。

- 「邪惡雙胞胎」（仿冒）

  「邪惡雙胞胎」是一個假冒的 Wi-Fi 連接，它欺騙用戶，令其相信這是合法連接，目的是進行仿冒詐騙攻擊以及利用數據交易找出保安漏洞。就「邪惡雙胞胎」的攻擊，攻擊者收集有關該合法存取點的資訊，然後設置其系統以仿冒該合法存取點。攻擊者使用比合法存取點更強的廣播訊號，讓無戒心的用戶連接到其存取點。

- 惡意存取點（未經授權的裝置）

  惡意存取點是未經網絡管理員明確授權所安裝的存取點。它可能造成中間人攻擊，讓網絡安全受到破壞。

Wi-Fi 訊號

- 「背負式」

  存取點的廣播範圍可以在建築物的牆壁和窗戶之外提供無線連接。如果未能妥善配置無線網絡，則在該存取點範圍內，任何人只要有已啟用無線功能的電腦，就可以使用該連接。這些用戶能夠進行非法活動，監視與擷取網絡資訊，或從網絡竊取檔案。

- 「戰爭駕駛」

  類似「背負式」，「戰爭駕駛」是指實體地搜索不安全的無線網絡或容易受到破壞的網絡。

- 拒絕服務

  拒絕服務是指一種攻擊，旨在剝奪某一個體的服務之可用性。攻擊者利用無線電干擾訊號，直接損害無線連接或設備，使它們保持忙碌。

- 竊聽

  竊聽是指秘密收聽通訊的行為。對於客戶端設備和存取點之間的網絡通訊，未經授權的監察容易導致通訊被竊聽，並且沒有實體攔截的跡象。

具有 Wi-Fi 連接的流動裝置

- 互聯網連接共用和橋接用戶端

  一個裝置若能分享互聯網連接或允許同時連接多個網絡，就可用於繞過網絡監察和保安控制。這可能會導致丟失數據或提供了保安不妥善的網絡進入點給攻擊者。

- 流動裝置被竊

  採取保護措施去避免丟失或盜去具有 Wi-Fi 連接的流動裝置是非常重要的。通過實體竊取流動裝置，攻擊者可以不受限制地接達裝置上的所有數據以及任何已連接的雲端帳戶。

5. Wi-Fi 網絡設置和操作的保安考慮

一般來說，有線網絡設置和操作的保安考慮亦適用於 Wi-Fi 網絡。具體來說，決策局／部門應制訂 Wi-Fi 保安政策，以及遵行本節就 Wi-Fi 網絡所描述的保安措施之作業模式。在計劃過程中，在 Wi-Fi 網絡的設置和操作方面若有考慮保安事宜，就會減少網絡暴露於較常見的攻擊。

5.1 設置 Wi-Fi 網絡的保安考慮

應部署保安措施和控制以保護 Wi-Fi 網絡。以下是一些相關的人員，如網絡擁有者、網絡管理員和終端用戶常見的保安考慮。

網絡擁有者

- Wi-Fi 網絡的用途

  應清楚說明 Wi-Fi 網絡的目的和功能要求。如果 Wi-Fi 網絡是獨立的，只供外部用戶接達互聯網，該 Wi-Fi 網絡須實體上與決策局／部門的網絡分開。應為不同類型的用戶和要傳遞的資料類型及其資料保安級別，分別指定 Wi-Fi 網絡的存取控制。

- Wi-Fi 保安策略

  應制定 Wi-Fi 保安政策，以處理無線網絡的所有使用選項，以及可傳遞的資訊類型。應定期檢討這項政策，以應付最新的科技及業務發展。該政策應包括但不限於定義 Wi-Fi 管理者的角色和責任、安裝和使用程序以及操作指引。

  例如，使用策略應訂明如當 Wi-Fi 功能不再使用時，就應關掉，並且不應分享或披露用於接達 Wi-Fi 網絡的加密金鑰或憑據。應分配獨立無線局部區域網絡供訪客。職員不允許設置自己的存取點。

- 數據保護和配置備份

  此項措施包括數據儲存時加密，安全的數據傳遞和定期備份所有在客戶端裝置和端點有用之資料，以及在網絡裝置內的配置檔案。

- 資訊科技保安風險評估和審計

  Wi-Fi 網絡須定期接受保安風險評估和審計。各決策局／部門須按在保安風險評估和審計中發現的任何保安漏洞，採取必要的補救措施。因應 Wi-Fi 技術的迅速變化，Wi-Fi 網絡的保安風險評估和審計須每年進行一次。

- 監測和預防

  這些措施包括記錄和審計網絡活動、漏洞掃描、有效的資訊發布機制和向所有工作人員提供關於 Wi-Fi 保安政策的保安意識培訓。應將活動記錄轉移到遠端記錄伺服器，並確保所有記錄的全面性和完整性。應定期審查和檢查記錄，以及發現任何可疑活動時進行分析。

- 保安事件處理

  決策局／部門需要遵守現行的資訊保安事件回應機制，將與 Wi-Fi 網絡相關的任何保安事件報告給政府資訊保安事件應變辦事處。還應定期更新該機制，以處理新的潛在保安威脅。決策局／部門還需要提供一個聯絡點，以便在緊急情況下，決策局／部門在短時間內關閉受影響的網絡。

- 保留清單並定義硬件棄置原則

  保持一個準確的 Wi-Fi 組件庫存，包括網絡交換機、路由器、互聯網閘道、存取點和其他相關組件，以確保只有授權用戶裝置才能連接到 Wi-Fi 網絡。一旦裝置遺失，應立即更改加密金鑰和服務設定識別碼。

  在硬件棄置策略中，當棄置所有硬件（包括任何 Wi-Fi 組件或裝置）時，應要求對裝置上的所有敏感資訊（如系統配置、預定的共用金鑰、數位憑證和密碼）進行清理。

- 定義修補程式管理原則

  定期測試和更新所有硬件、設備和軟件程式的最新韌體和保安修補程式，以防止因疏忽而造成的漏洞及惡意攻擊。

<u>網絡管理員</u>

網絡管理員應考慮在多方面採取以下保安措施，以保護 Wi-Fi 網絡的可用性以及資訊的機密性。

- Wi-Fi 網絡容量

  為確保 Wi-Fi 網絡的可用性，應考慮 Wi-Fi 網絡用戶數量的多少和應用程式的類型（例如，語音/視像會議或網上瀏覽），評估無線連接的容量。

- 存取點的實體保護和位置

  無線訊號通常不會覆蓋在特定區域中。過度覆蓋可能讓惡意用戶對網絡構成重大的威脅和增加攻擊的機會。因此，存取點的位置和無線訊號的強度應經過小心設計，在實際可能的情況下使在設計區域之外不提供無線訊號。例如，應考慮將存取點安裝在遠離窗戶或門的地方，以防止來自公共地方的區域網絡竊聽。還應避免對同地域無線網絡的相互干擾。建議進行場地勘察，以確定 Wi-Fi 基礎設施的覆蓋範圍、存取點的數量及其位置和訊號覆蓋範圍和品質。

  網絡設備（如存取點）應安裝在具有嚴格實體保安控制的設施中，以防止盜竊、破壞或篡改，特別是對於放置在開放區域的存取點。應考慮將存取點安裝在天花板上，並鎖定配線設施。此外，應考慮使用任何鎖定機制來實體限制對存取點的電源按鈕、重置按鈕或埠（例如通用串列匯流排）的接達。

- 網絡分段

  應為訪客、應用開發和內部網絡進行 Wi-Fi 網絡分段。存取點覆蓋區域的分段還可以平衡 Wi-Fi 網絡上的負載，從而最大限度地降低可用性的風險。此外，應限制 Wi-Fi 和有線網絡之間的互連。應採用分段 Wi-Fi 網絡之間的存取控制（例如防火牆、埠/應用程式/媒體存取控制的位址過濾）。

- 傳輸標準

  Wi-Fi 網絡的傳輸標準是基於 IEEE 802.11 標準，如 802.11g、802.11ac、802.11i、802.11n 和最新標準 802.11ax。從保安角度來看，802.11ax (Wi-Fi 6) 與 Wi-Fi 保護接入 3 (WPA3) 協定引入增強的認證和加密功能。

  Wi-Fi 6 是 Wi-Fi 技術的最新標準。它的設計是為了回應全球越來越多的無線裝置和小工具。與之前的版本 (802.11ac) 相比，它的功能和特點都改進了。應考慮使用最新版本的通訊協定 (如 IEEE 802.11ax) 來構建 Wi-Fi 網絡，尤其是物聯網系統，它可能連接多達數千台將會要連接的裝置。

Wi-Fi 保護接入 3 (WPA3) 有兩種模式，即 Wi-Fi 保護接入 3 (WPA3)-企業模式和 Wi-Fi 保護接入 3 (WPA3)-個人模式。建議使用 Wi-Fi 保護接入 3 (WPA3)-企業模式，因為它提供了增強的保安功能來構建 Wi-Fi 網絡。若使用 Wi-Fi 保護接入 3 (WPA3)-個人模式，應定期更改加密金鑰。

- 互聯網通訊閘

  互聯網通訊閘的保安措施包括防火牆、入侵檢測系統和入侵防禦系統，用於檢測和防止任何可疑活動。應安裝防火牆以防止網絡攻擊和入侵。視乎情況，決策局／部門還應掃描/監察網絡通訊，並篩選可疑的協定、資料包和內容。

- 管理系統

  位於用戶區域的合法 Wi-Fi 存取點，應啟用認證。應實施用戶身份認證，特別是無線裝置。應安裝主機級的防火牆和抗惡意軟件程式的防護。還應在 Wi-Fi 和有線網絡上安裝入侵防禦系統，以檢測任何可疑活動。

- 存取點的配置

  存取點是 Wi-Fi 網絡的核心組件。需要為存取點制定基準保安配置標準，以採取適當措施保護它們。建議的控制項包括但不限於以下各項：

  - 更改存取點的預設設定。例如更改預設管理帳戶和密碼，禁用存取點上的不必要或不安全的服務、協定和未使用的管理界面。
  - 確保所有存取點具有嚴謹、獨一無二的管理密碼，並定期更改密碼。
  - 將預設服務設定識別碼 (SSID) 的名稱更改為適當且不顯眼的名稱 (例如，Wi-Fi.HK)。SSID 的名稱應防止披露網絡的系統詳細資訊，如產品名稱/型號。
  - 如果獨立 Wi-Fi 網絡僅供獲授權的預設裝置使用，則不要廣播 SSID。如果需要廣播 SSID，則只能覆蓋在指定的範圍內。
  - 在用戶區域中對合法存取點進行認證。

- 用戶端裝置

  應隔離個別用戶端避免點對點通訊，以防止惡意軟件攻擊。應使用具有 Wi-Fi 防禦的流動裝置的客戶端數碼證書，以便只允許授權裝置存取部門網絡或資源。

5.2 Wi-Fi 網絡運作的保安考慮

就 Wi-Fi 網絡的不同組件，各方人員（如網絡管理員和用戶）應採取以下 Wi-Fi 網絡操作的保安措施。

網絡管理員

網絡管理員應在用戶端裝置、管理系統和連接中實施以下技術安全措施。

用戶端裝置

網絡管理員應保護部門網絡，避免受來自用戶端裝置的惡意軟件程式感染，並限制只供已獲授權的用戶端裝置使用。定期變更存取點的加密金鑰。

管理系統

應記錄用戶活動和監察事件，以檢測任何惡意活動並作進一步調查。應該修補存在網絡裝置的保安漏洞，因這些保安漏洞可能會被入侵者利用；定期掃描 Wi-Fi 訊號，以偵測惡意存取點是否已安裝在 Wi-Fi 網絡的覆蓋範圍內；和偵測可疑網絡流量和惡意攻擊。

用戶端裝置與連接

就與用戶端的連接，終端用戶應把經無線方式傳遞的數據加密，以保護資料的機密性。用戶端裝置應避免連接不可信任的/不知名的存取點，和不要以 Wi-Fi 熱點或臨時模式聯網，分享或擴展政府內部網絡。

終端用戶

以下是終端用戶在存取 Wi-Fi 服務時的最佳實務 —

設置

- 將預設的互聯網連接設定為手動模式，而不是自動模式。
- 關閉點對點/臨時模式聯網。
- 啟用用戶端裝置電源接通時的登入，以便接達該裝置時要求密碼。
- 安裝並啟用個人防火牆、防病毒軟件和防間諜軟件。

使用

- 不要讓用戶端裝置無人看管。
- 未使用時關閉無線連接。
- 驗證強制網絡門戶的證書，以確保它不是一個假的門戶。
- 不要連接到不認識的 Wi-Fi 網絡。
- 當有可疑活動時，把 Wi-Fi 網絡連接斷開。

維護

- 當用戶端裝置的應用程式和驅動程式有保安修補程式時就應採用。
- 定期備份數據。
- 在棄置之前，刪除用戶端裝置上的所有數據和敏感配置資訊，如 SSID 或加密密鑰。

5.3 通過 Wi-Fi 網絡進行遠程接達

若資料透過 Wi-Fi 傳遞但未獲保護便容易受到攻擊。在無線裝置之間傳遞的敏感資訊如未加密（或使用的加密技術較弱），就可能會被截取和披露。因此，傳送敏感資訊時須採取保安措施。

對於經無線通訊接達敏感資訊時，應考慮將所有無線接達視為不可信任的連接。因此，以無線通訊接達內部系統時，只能授予透過指定的通訊閘道（例如虛擬私有網絡閘道），並且有妥善的認證、加密和實施了用戶級別的接達控制和記錄。

必須推行足够的認證和加密措施，來進行遠程及經 Wi-Fi 至內部網絡的接達。當連接到政府內部網絡時，決策局／部門必須採用安全的渠道（例如虛擬私有網絡、通過保密超文本傳輸規約的虛擬私有網絡），並通過雙重認證。以下是一些建議措施：

- 更新 Wi-Fi 連線端點（例如流動裝置）上抗惡意程式軟件的定義至最新版本。
- 安裝最新的保安修補程式。
- 開啟主機級的防火牆或入侵防禦系統。
- 開啟端點裝置上儲存加密的功能。
- 在虛擬私有網絡客戶端接達的清單上註冊端點裝置。
- 虛擬私有網絡帳戶採用嚴謹密碼。
- 開啟使用權標或一次性密碼的雙重認證。
- 啟用閒置超時（例如 10 分鐘）功能以中斷虛擬私有網絡連接。
- 為所有連接 Wi-Fi 的虛擬私有網絡，開啟紀錄功能。
- 如果媒體接達控制地址過濾功能已啟用，則註冊端點的媒體接達控制地址。

6. 新興技術

6.1 5G 簡介

5G 是指第五代的流動通訊技術，它是由國際電信聯盟為發展新一代流動科技而制定的。5G 的流動技術功能超越了 4G。5G 流動技術的最高數據傳送速率可達到每秒 20 兆數元，然而用戶所體驗的數據速率可能因流動裝置所處的環境而有所不同。由於 5G 網絡是建立在現有電訊網絡之上的，在可預見的將來，預期 5G 的網絡基礎設施仍會繼續用於提供 3G/4G 服務。

5G 的新容量和特性

物聯網應用程式的促成

5G 網絡的下載和上傳速度顯著提高。5G 網絡的延遲 [1]也減少了。5G 還使大量機器之間的通訊能夠進行，它允許更多的裝置，特別是物聯網裝置，在一個小範圍內連接到網絡。

以軟件為基礎和虛擬化技術

5G 是透過網絡功能虛擬化、軟件定義網絡和網絡切片，在網絡管理功能上採用新的軟件程式 [2]和虛擬化技術 [3]。這些技術使 5G 能夠支援共存，以及隔離不同需要類型的 5G 網絡服務的應用程式，但這些應用程式能同時共用相同的基礎架構。例如，流動寬頻服務需要更高的數據傳送速率，而智能汽車應用需要快速回應（低延遲）與感測器之間的數據通訊。

6.2 5G 流動網絡服務的威脅與網絡漏洞

5G 流動網絡服務及其底層基礎設施是由公共通訊網絡營運商提供。與其他通訊網絡（如 4G、Wi-Fi 或電話線）一樣，5G 網絡視為不可信任的通訊網絡。通過任何公共通訊網絡傳遞資訊都可能會面臨保安風險，因為惡意攻擊者可能會利用通訊網絡的漏洞獲取保密資料，甚至闖入政府網絡。公共通訊網絡的威脅同樣適用於 5G。此外，以下將詳細闡述 5G 特有的一些威脅。

[1] 延遲是指從基站發射數據到目標裝置(例如流動電話)接收數據之間的時間間隔。

[2] 軟件定義網絡和網絡功能虛擬化的部署是透過允許對傳統網絡架構進行分區，從而提供更大的網絡靈活性。

[3] 通過切片方式，公共網絡營運商經基礎設施為客戶提供專用虛擬網絡。網絡切片的用戶體驗與實體上獨立的網絡是相同。

新增 5G 應用程式與網絡技術的漏洞

由於 5G 網絡提供更闊的頻寬和更高的數據傳輸速度，它促進了能利用這些先進科技優勢的創新應用程式，得到廣泛增長。隨著新應用程式的到來，但也帶來一些保安風險。此外，5G 架構涉及各種功能層，並且通過基於軟件和虛擬化技術實現。但是，使用這些新軟件技術也意味著帶來網絡操作中的保安漏洞。如果決策局／部門的網絡未妥善連接和保護，5G 基礎架構軟件的新保安漏洞就可能會影響決策局／部門。

5G 裝置的威脅層面增加

5G 網絡有能力支援更多的網絡連線，從而允許大量類型的裝置，尤其是物聯網裝置同時地相互連接。由於在短時間內推出市場和成本考慮，有些連接上網絡的裝置可能只達到較差的保安標準和功能，這能導致威脅層面擴大。如果某一個已連接上網絡的裝置存在漏洞，惡意攻擊者可能會入侵並且控制該裝置。再者，攻擊者可以危及網絡上其他的裝置，並執行對整個網絡的攻擊。

具有 5G 連接的裝置的配置錯誤

隨着採用 5G 的流動裝置或物聯網裝置日益增多，這些裝置可能內置 5G 連接功能。由於 5G/物聯網技術可以方便地實現動態連接，用戶應注意裝置更容易受到各種潛在風險的影響。例如，用戶可能會將物聯網裝置連接到政府網絡，並無意中對外披露敏感資料。此外，攻擊者可以利用 5G 功能來進行其他攻擊，如惡意軟件程式傳播，分散式拒絕服務攻擊，仿冒詐騙和垃圾郵件攻擊等。

流動裝置，例如手提電話、平板電腦和筆記型電腦，一般透過通訊網絡（包括 5G）連接到互聯網。如果沒有適當管理保安風險，保護措施不夠和未能有效實施，就會增加機會令到資料、流動裝置和相關通訊網絡容易遭到未經授權的接達、修改、丟失、被盜或泄露，甚至流動裝置也很有可能成為發起攻擊網絡的一部分。

5G 基站的風險因素

由於 5G 基站的運作是使用高頻率訊號，所以 5G 基站的密度會比現時蜂窩式電訊網絡為高。因此，流動網絡營運商可能要求將 5G 基站和天線單元安裝到政府處所，以提供更好的 5G 網絡服務。當這些非政府擁有的設備在政府處所內未得到妥善管理，而這些流動網絡營運商的人員或承辦商也不是由政府直接管理，這可能會給政府帶來保安風險。

6.3 使用 5G 流動網絡服務的保安注意事項

公共 5G 網絡的部署不應與其他傳統網絡（如 4G、3G 和固網電訊）有重大區別，並應假定所有公共或流動網絡都不可信任。通過公共或流動網絡進行的任何政府通訊，都應根據保密資料分類受到額外保安措施的保護，例如加密、身份認證、接達控制等。此外，在採用新技術後，所有相關的持份者應關注新技術可能帶來的資訊保安威脅，並及時採取有效措施，包括採用最新標準或安裝修補程式。

新的 5G 應用程式與網絡技術

5G 網絡

就將公共網絡連接到部門網絡的保安考慮，應參考《互聯網通訊閘保安實務指引》。例如，決策局／部門應要求系統集成商或流動網絡營運商提供保安控制，包括但不限於接達內部網絡時安裝保安閘道或非軍事區；傳輸數據時加密；監察系統和網絡，防止任何惡意攻擊，如分布式拒絕服務攻擊和中間人攻擊。決策局／部門還應啟用保安監察和管理解決方案，以便更好地監控網絡和任何攻擊。

就新的 5G 網絡虛擬化技術，依靠這些新網絡技術的應用意味著網絡的運作有可能存在漏洞。儘管這些新技術的許多保安責任都是由流動網絡營運商或虛擬化平台擁有者承擔，但決策局／部門應注意這些易受攻擊點所引致的漏洞，並要求系統集成商或服務提供者在涉及 5G 應用程式時提供保安控制。決策局／部門應通過訂閱保安新聞、警報、報告和其他資訊保安出版刊物，清楚地瞭解此類有關 5G 連接而出現新的保安威脅和相關風險，以便決策局／部門能夠儘早收到警報並針對此類威脅實施適當措施。

下面重點介紹 5G 網絡的部署和管理相關的一些注意事項：

- 如果沒有預計連接 5G 網絡，應停用網絡設備中不必要的內置 5G 功能。
- 制定在業務中採用 5G 服務的營運計劃，包括但不限於評估 5G 應用和網絡技術的成熟度、資產管理的考慮、接達控制、實體保安、操作保安、通訊保安、加密控制、與外部網絡活動的記錄以及外判、應用程式開發、業務連續性、事件管理和法規遵循性方面的考慮，以及決策局局長／部門首長的批准。
- 將連接到 5G 服務的網絡分段與其他網絡分段隔離。如果網絡分段上的一個經 5G 連接的主機受到損害，這樣就會將攻擊層面減少。
- 可以將敏感和內部子網絡與一般網絡分離，以增強動態網絡連接下的保安管理。
- 考慮聘請在 5G 網絡方面具有專業知識的獨立審計師，來審查和檢查連接到 5G 網絡的配置和實現。

5G 應用

5G 促進創新應用的發展，特別是物聯網和流動應用。若在設計層面時已考慮保安要求，就能識別應用程式系統的潛在風險，並在專案的早期階段進行適當的補救。建議各決策局／部門參考《流動保安實務指引》的第 5 節「流動應用程式開發保安」，該章節為開發用於業務的流動應用程式，提供指導說明；以及《物聯網保安實務指引》，該指引重點介紹採用物聯網以及各種相關保安領域時，常見的保安考慮和良好作業模式。對於部署使用 5G 連接的應用程式，應遵循在政府保安文件內就一般應用程式所訂明的保安要求。以下列出數項要點供各決策局／部門考慮：

- 留意在保安方面的技術發展，並研究和評估保安機制和功能，以選取能符合保安要求的應用。
- 只採用必要和安全的功能。不啓用不需要的功能，尤其是物聯網裝置。
- 避免收集和儲存超過要求所需的敏感資料。
- 為保護敏感資料，確保資料在不同端點和傳輸過程中受加密保護。
- 啟用認證和授權，以確保服務的使用者和提供服務者也是獲授權的。

5G 裝置

事實上適用於流動裝置的一般保安實務、措施和控制，亦適用及有效地保護 5G 裝置。建議決策局／部門參考《流動保安實務指引》第 4 節「流動裝置保安」，該章節提供在業務中使用和採納流動裝置的保安指引。這些措施的例子包括平台和裝置的獨特識別，反檢查機制，以防止裝置的任何錯誤設定，接達裝置的控制，儲存和傳輸加密，以及加密金鑰的有效性和其在失效前的續期。用戶、應用程式開發人員或管理員分別負責保護其流動裝置、數據資產和相關資訊科技基礎設施。

應定期提供培訓，以增加用戶對正確使用 5G 裝置的認知，其方式與流動裝置或物聯網裝置類似。以下是培訓中一些建議的內容，以提高他們的意識。

- 5G/物聯網技術促進動態連接，用戶應注意其裝置更容易受到各種潛在風險的影響（例如，將私人擁有的物聯網裝置連接到載有敏感政府資料的網絡）。
- 用戶應該知道，使用有保安漏洞以及保安設置較差的裝置，會產生更大的網絡攻擊風險。
- 用戶應部署有技術支援（如提供保安裝置修補程式）的設備，以便保持該設備的保安。
- 用戶應仔細檢查裝置的網絡設定，並僅允許必要時連接到 5G 網絡或設備。
- 用戶不應在未獲批准前將其 5G 裝置直接連接到部門網絡。

5G 基站

在頻譜方面，5G 運作所需的頻率高於 4G。由於高頻訊號的穿透能力較低，所以設置 5G 基站和天線單元時，就需要較密集和近距離的，以令所提供的服務能有可接受的表現。如有需要將基站安裝在政府處所內，應考慮採取下列保安措施：

- 在安裝前，應明確界定政府和流動網絡營運商的擁有權、角色和責任。流動網絡營運商會為處理這些設備而提供相關的項目和服務。因此應就管理該些項目和服務，制定適當的保安程序。
- 對於啟用 5G 的網絡設備，應建立適當的實體接達控制，並且應指定工作人員來監察。
- 應制定適當的實體環境的保安程序，以控制和記錄以下工作：安裝、日常維護、更改配置和所有由工作人員為 5G 網絡組件所進行的檢查。工作人員的例子有外部顧問、承建商和臨時工作人員。
- 向流動網絡營運商闡明營運商的高級技術人員（如特許工程師）已批准和驗證將會安裝在 5G 基站的更新/修補程式。
- 5G 基站或相關設備並不是資訊通訊科技基礎設施中常見的網絡設備。若果有不確定的情況，在安裝前請先向電訊工程師，就其專業領域諮詢保安建議。

事故處理

應檢討保安事故處理程序及進行必要的修改，以處理各種可疑活動的情況，例如 5G 網絡因漏洞而受到損害和基站遭到破壞。此外，記錄應受到完全控制，並得到充分的保護。如果發生了保安事故，不論來自外部或內部攻擊的，系統記錄和使用記錄對於調查是關鍵的。

*** 完 ***