數字政策辦公室

資訊保安

流動保安

實務指引

[ISPG-SM03]

第 2.1 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	本文件由"流動裝置保安實務指引 1.0" 更名為"流動保安實務指引 1.1"。並增加關於資訊科技保安管理和流動應用程式開發保安的新章節及維持與其他實務指引有一致的參考。	整份文件	1.1	2018 年 7 月
2	增加本文件以下的內容： 流動裝置管理指引； 流動應用程式的數據保護； 開發安全流動應用程式的良好作業模式；以及 獲授權流動應用程式的評估指引	12; 14; 20-21; 28,30,31; 附件 C	2.0	2021 年 6 月
3	將「政府資訊科技總監辦公室」更改為「數字政策辦公室」		2.1	2024 年 7 月

目錄

1. 簡介

流動裝置日漸普及，用戶可隨時隨地存取資訊，這改變了使用互聯網的模式，同時亦對日常運作帶來了新風險。儘管流動裝置和其上安裝的流動應用程式（應用程式）帶來了便利並提高了效率，但保護不足之流動裝置或不安全編寫之流動應用程式對使用者會帶來風險，也可能令應用程式擁有者/開發者遭受資料泄漏或聲譽受損的威脅。考慮到流動裝置的高度便携性、無線連接功能所帶來的額外風險，及多樣化之流動應用程式的開發技術的特點，我們編寫本文件，旨在為決策局／部門提供安全使用流動裝置和開發流動應用程式的指引。

1.1 目的

本文件旨在為決策局／部門提供管理及使用流動裝置以及安全開發流動應用程式常見的保安考慮及良好作業模式。**第 4 章**將介紹流動裝置使用和管理的良好作業模式，適用於有關使用和採用流動裝置及相關管理解決方案的員工。**第 5 章**將介紹流動應用程式開發保安的良好作業模式，適用於參與相關開發周期的人員。

本文件應與政府的保安要求和文件，包括《基準資訊科技保安政策》[S17]，《資訊科技保安指引》[G3]及其他相關程序與指引一同使用。另外，決策局／部門在採納流動裝置方案前，應根據業務需要，評估保安風險。決策局／部門應細閱本文件所介紹的保安措施及良好作業模式，為自己的流動裝置方案進行合適的保護。

本文件內容屬概括性質，可涵蓋不同種類及作業平台之流動裝置的種類及作業平台。根據政府保安文件中流動裝置的定義，「流動裝置」指可儲存及處理資料的便攜式運算及通訊裝置，例子包括便攜式電腦、流動電話、平板電腦、數碼相機，以及數碼錄音或錄像裝置。讀者應按其環境，考慮及選擇適合的保安措施及良好作業模式。

1.2 參考標準

以下的參考文件為本文件在應用上的參考：

- 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
- Information technology – Security techniques – Governance of information security, ISO/IEC 27014:2013
- Information technology – Security techniques – Storage security, ISO/IEC 27040:2015

1.3 定義及慣用詞

本文件採用《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	
無	無

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。

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. 流動保安簡介

今時今日，流動裝置為用家帶來極大的方便，亦對業務運作十分重要，但亦帶來保安問題，例如流動應用程式增加資料遺失的風險。本節集中介紹應對常見的保安問題的保安措施及良好作業模式。決策局／部門宜根據本身的業務需要及環境考慮保安措施及良好作業模式。

3.1 流動科技面對的威脅

流動裝置的主要威脅來自裝置本身、網絡連接（例如流動通訊網絡和互聯網）及流動應用程式。與辦公室的工作站相比，流動裝置通常在室外或路上使用，在這些地方它們更容易遭受威脅和遺失。以下是一些流動技術的相關保安風險：

流動裝置

- 使用缺少實體保安控制的裝置

  流動裝置往往是體積細小，一般用於辦公室控制範圍以外的各種地方，例如員工家中、咖啡店、酒店及會議場地等，其流動性令裝置比其他裝置更容易遺失或被盜，令資料外泄的風險增加。

- 使用保安控制不足的流動裝置配件

  流動裝置通常都備有相機及麥克風。不恰當的錄影、拍照及攝影可導致保安問題。另外，若流動裝置未有得到適當的保護，未獲授權人士便有可能獲取裝置內的敏感錄影、錄音或照片。

- 使用不可靠的流動裝置

  很多流動裝置，尤其是私人擁有的裝置，未必可靠。使用已越獄或根權限被破解的流動裝置，會導致更多的保安風險，原因是內建的保安限制已被繞過。

- 缺乏對敏感資料的保護

  流動裝置用於儲存敏感資料，包括個人資料、照片和聯絡人名單。載有敏感資料的文件亦有可能下載和儲存在決策局／部門批准和管理的流動裝置中。為了防止由於網絡攻擊或流動應用程式過度收集數據而導致數據泄露，這些敏感資料需要使用流動裝置內置功能或獲授權的保安工具進行加密保護。

- 不安全的屏幕上鎖配置

  鎖定屏幕是第一道防線，以防止未經授權接達流動裝置及其中所儲存的資料。正確的鎖定屏幕配置（例如嚴謹密碼）可以保護裝置免

遭未經授權接達和數據泄露。此外，某些流動應用程式可能仍會在鎖定的屏幕上顯示推送通知，例如訊息、由應用程式發出的通知和新收到的電子郵件。如果通知的內容包含敏感資料，這些敏感資料有可能被一些未經授權的人士看到。

- 使用公共的流動電話充電設施

  一些購物中心和公共交通工具都有提供公共流動電話充電設施。如果公共的流動電話充電站（尤其是帶有 USB 充電接口）被入侵，則惡意軟件將通過該充電站安裝到裝置上，從而竊取裝置內的敏感資料。故此，應盡量避免使用可疑的流動電話充電設施。

網絡

- 使用不可信的網絡

  流動裝置基本上是使用非機構自設的網絡接達互聯網，如外部 Wi-Fi 及流動電話網絡。這些網絡容易被竊聽，令敏感資料有機會外泄。

- 使用不安全的通訊技術

  與主要依靠局部區域網絡或辦公室無線網絡的辦公室內工作台相比，流動裝置能夠廣泛利用各種通訊技術，例如藍牙和近距離無線通訊作數據連接。每種通訊技術都有其保安風險。若敏感資料於通訊媒介中遭攔截，則會導致保安事故。

應用程式

- 使用獲授權的應用程式

  為了保障流動裝置安全，流動裝置上的應用程式應只供業務之用。供個人使用的流動應用程式，例如遊戲、線上支付、在線購物等，除非有充分的理由，否則應盡量避免安裝在決策局／部門所提供的流動裝置上。

- 不可信的流動應用程式的風險

  流動裝置的設計令使用者能從流動應用程式商店中輕易找尋、獲取、安裝及使用第三方的應用程式。但這卻帶來明顯的保安風險，尤其在不設保安限制或其他制約的流動裝置平台及流動應用程式商店所發佈的由第三方開發的應用程式。

- 顯示流動裝置位置的風險

  定位服務是社交媒體、導航及其他流動為主的應用程式普遍會使用，為裝置和其使用者確定位置的服務。已啟用定位服務的流動裝置會較有機會成為被攻擊的目標，因為這會令潛在攻擊者更易知道使用者及流動裝置的位置，然後將位置資料結合其他來源的資訊，從而發動如魚叉式仿冒詐騙的攻擊。

- 不受控制接達流動裝置傳感器／配件的風險

  流動應用程式可能導致智能電話和平板電腦內置相機等桌面電腦不常見的傳感器／配件，在不受控制的情況下被接達。這樣有可能構成針對性攻擊的風險，例如一些在公共場所展示的惡意二維條碼或 QR 碼。

- 地理標記的風險

  流動裝置通常有地理標記功能，能自動將地理資訊（即位置和 GPS）標記到裝置所拍攝的照片和其他媒體上。因為照片擁有人的姓名和所拍攝照片的地理位置，會在無意間被不知名人士和潛在攻擊者收集，增加了個人私隱泄露的風險。

- 泄漏個人資料的風險

  流動裝置的聯絡人名單和通訊錄被廣泛用於儲存個人資料，例如姓名、電話號碼、地址、出生日期、電郵等。一些流動應用程式可能要求接達聯絡人名單或通訊錄的權限以支援該程式的操作。如果敏感資料（例如個人識別碼(PIN)、帳戶名稱、帳號或密碼）儲存在聯絡人名單或通訊錄中，便可能構成經流動應用程式泄露這些敏感資料的高風險。

開發流動應用程式

與使用流動應用程式相比，開發流動應用程式時需要處理額外的保安風險。開發人員可參考開放網路應用程式安全計劃（OWASP）十大流動應用程式開發風險(Mobile Top 10)，以了解流動應用程式開發面臨的主要風險。決策局／部門應參考這些常見的保安風險，並避免在編寫程式時出現這些問題。決策局／部門亦應檢討及界定其應用程式的保安要求，以減低風險，避免設計上的保安漏洞。OWASP 提到的有關流動應用程式風險歸納如下：

- 不當使用平台

  這個潛在威脅源於程式誤用平台功能和沒有採用平台所提供的保安控制措施（例如 Android 意圖、平台權限、不當使用生物識別功能或有關流動作業系統的其他保安控制措施）。不當使用平台功能可能令系統蒙受風險（如跨網址程式編程）。

- 使用不安全的數據儲存

  當軟件開發者假設用戶或惡意軟件不能接達流動裝置的檔案系統及裝置的敏感資料時，數據儲存漏洞便可能會出現。通過流動惡意軟件、經修改的應用程式或取證工具，可能會導致數據遺失或程式中的敏感資料遭提取。

- 使用不安全的通訊

  不安全的通訊會構成應用程式所傳輸的數據暴露風險，可能導致敏感資料外泄。有關問題的成因可能是不良的交握式通訊、不正確的保密插口層（SSL）版本、使用不合格的交涉協議及以純文字格式傳輸敏感數據資產。

- 使用不安全的認證

  攻擊者可能會破解密碼、密碼匙或認證權標，以假冒其他用戶的身分。有關問題的成因可能是欠缺或沒有妥善推行帳戶認證機制，以及不當的對話管理。

- 使用不安全的授權

  一些流動應用程式會在用戶認證後自動給與一些權限。這些授權有時會被錯誤地過度擴展，提供流動應用程式不應該有的權限。如果攻擊者得到應用程式的特別權限，便可能導致未獲授權而接達敏感資料的情況。

- 使用不足的加密

  如果數據未加密或不當使用加密功能進行加密，攻擊者會盜取或接達保護欠佳的數據。

- 客戶端程式碼層次的錯誤

  程式碼層次的錯誤可能產生漏洞（如緩衝區滿溢和記憶體外泄），讓攻擊者可對流動應用程式作出惡意輸入。這可能會引致執行外部程式碼或遠程伺服器拒絕服務（DoS）。

- 使用被竄改的程式碼

  攻擊者可能會以存放於第三方位置的惡意應用程式竄改該流動應用程式。攻擊者亦可能通過仿冒詐騙攻擊誘騙用戶安裝應用程式。

- 不足以防範程式碼還原工程

  攻擊者可能會分析核心二進制程式碼，找出其源碼、源碼庫、算法和其他資產，從而利用漏洞、收集敏感數據或盜取知識產權。

- 不當處理外部功能

  在開發階段，開發者可能會建立一些隱藏的後門程式或功能，以便為應用程式除錯。如後門程式在推出的版本仍然存在，攻擊者便可利用這些後門程式作出惡意行為。

4. 流動裝置保安管理

本章介紹如何在流動裝置使用周期內保護裝置，以及流動裝置管理解決方案的常見保安功能。本章適合於使用和採用流動裝置及相關管理解決方案的用戶和管理員。

4.1 流動裝置使用周期

與其他資訊系統相似，流動裝置在整個使用周期中包括三個主要階段 – 提供、使用和停止使用。以下小節將討論如何在周期的各個階段保護流動裝置的一些良好作業模式。

4.1.1 流動裝置的提供

當決策局／部門考慮於業務中採用流動裝置時，應了解自己對流動裝置的需要，以及知道流動裝置方案如何支援本身的業務。應訂立流動裝置保安政策，當中列明使用流動裝置的業務及保安要求，並訂定適當的流程和程序以提供流動裝置。以下是一些考慮事項：

- 審批流動裝置的機制及獲批准的流動裝置的種類。
- 每種流動裝置上所容許的數據保密級別。敏感資料不可儲存於私人擁有的流動裝置內。
- 確保基於數據保密級別的控制機制符合政府的保安要求。
- 根據操作需要，界定和備存授權軟件列表，包括免費軟件、開源軟件和程式庫。
- 在職員轉職或離職時，確保相關程序能確保適時清除儲存在流動裝置上的敏感資料。

決策局／部門應覆檢及按所需調整修改流程，使供應階段能具有以下良好作業模式：

- 制訂符合運作及保安要求的型號清單。
- 在提供新型號的流動裝置前進行風險評估，並推行持續風險監察機制，以評估流動裝置所涉及的風險轉變或新風險。
- 按可行性安裝保安控制工具，例如流動裝置管理[1]、數據遺失防護、個人防火牆軟件及抗惡意軟件。應於決策局／部門的強化程序中列出所使用的工具。

[1] 流動裝置管理是一個（或一系列）應用系統，為流動裝置如電話及平板電腦提供政策、庫存、保安及服務等方面的管理功能。就流動裝置管理詳情，請參閱本文件第 4.2 節－流動裝置管理方案。

- 在決策局／部門所擁有的流動裝置中只使用獲審批的應用程式。獲得決策局／部門委任人士授權後，用戶才可安裝第三方應用程式。
- 為流動裝置進行保安強化處理，將已強化的裝置交付用戶。
- 向用戶發放使用政策，並獲得用戶收到有關使用政策以及狀態良好的流動裝置的確認。該確認可以是已簽署的協議或電郵回覆。
- 定期向用戶發放保安提示，以提醒他們採用保安良好作業模式。
- 啟用開機密碼功能。
- 根據決策局／部門的部門保安要求，執行最起碼密碼長度及複雜性的要求。
- 設定流動裝置在閒置一段時間後自動鎖上。
- 啟動當多次連續輸入錯誤密碼後，數據自動刪除的功能（若有此功能）。決策局／部門應按其運作的需要，訂立連續錯誤嘗試的實際次數。亦應啟動遙距清除功能，當裝置遺失或被盜時仍能保護資料。此外，應仔細選擇清除方案，以確保刪除的敏感資料不能被恢復。
- 在可行的情況下，為流動裝置的所有儲存器啟動加密功能，可於裝置層面、全磁碟層面，或檔案層面啟動加密功能。
- 考慮使用多重認證機制，例如在使用虛擬私有網絡之同時使用數碼證書及密碼。
- 備存資產追蹤資訊，例如序號、檢查裝置上的應用程式及監察有關資料作審計之用。
- 流動應用程式權限。為了最大程度地減少安裝流動應用程式後受到損害的風險，流動裝置的用戶應採用「最小權限」原則，以最少系統權限和接達權限執行應用程式，從而使攻擊者無法接達其他應用程式（例如瀏覽器、聯絡人名單）或流動裝置的功能。
- 在安裝流動應用程式時，用戶應先閱讀資料披露、私隱政策聲明或同等資料的內容，並充分了解權限的保安風險，然後才按“我同意”或“允許”。通常應用程式要求的某些權限（例如聯絡人、麥克風和位置訊息）未必是核心功能所需要的，可以通過流動裝置上的應用程式權限關閉。

決策局／部門應根據政府保安要求及流動裝置保安政策，制定流動裝置保安強化程序，以執行保安配置。所有流動裝置在交予用戶前，均應依照保安強化程序加以強化。有關保安強化配置的範本，請參閱附件 A。

4.1.2 流動裝置的使用

即使在供應階段推行保安控制，人和程序仍然是保持流動裝置安全的兩大重要因素。因此，本節重點介紹流動裝置在持續的管理及使用中的良好作業模式。

4.1.2.1 管理員

管理員應跟從以下良好作業模式：

- 留意保安消息，例如保安警報或應用程式的新版本，以檢查流動裝置操作系統和流動應用程式的可用更新和／或保安修補程式；並及時採取適當的變更管理，例如將流動應用程式更新為最新版本。
- 如果流動應用程式已終止支援或不再使用，用戶應立即卸載該應用程式，以防止因該應用程式的保安漏洞而受到攻擊。
- 於流動裝置上安裝已經驗證的更新及／或修復程式。
- 定期檢查流動裝置以確認保安措施被執行。應檢測及限制使用已越獄、根權限遭破解及被入侵的裝置。
- 在可行的情況下，啟動流動裝置中的加密功能。
- 備存決策局／部門的流動裝置庫存記錄，記錄要包括裝置使用者資料及已安裝的應用程式的清單。有關清單應由決策局／部門指定人員保存。

  關於軟件特許使用權，決策局／部門必須負責定期保存、更新和管理所有軟件和流動應用程式特許使用證的記錄，並確保為所有已購買、正在使用和已棄置的軟件和流動應用程式保存最新的記錄，與現存特許證相符。至於軟件的機構特許使用權，必須確保已安裝的軟件數量不超過所購買的軟件數量。

- 決策局／部門應定期檢查軟件和流動應用程式庫存，以確保所有軟件均有特許使用權，以及沒有使用未獲授權的軟件或流動應用程式。

4.1.2.2 流動裝置用戶

用戶應遵從使用政策及保安提示，包括但不限於以下：

不要事項：

- 除已獲批准，否則不要修改流動裝置的設定。
- 不要嘗試使用未經授權的工具為流動裝置越獄／破解根權限或損害流動裝置操作系統，否則可能會帶來不能預計的保安風險及令保養服務失效。
- 不要容許不明或不可信的來源經無線連接到裝置。
- 不要開啟或接達來自具誤導性、可疑或不可信來源的社交媒體、即時通訊訊息、短訊服務、多媒體訊息服務或電郵內的連結。

- 不要從不明或不可信的來源下載程式和內容，以及安裝流動應用程式。
- 不要在流動裝置上安裝非法或未獲授權的軟件。
- 當流動裝置連接政府內部網絡時，不要直接接駁(如：經流動電話網絡)至外部數據網絡。
- 不要使用公共打印機。
- 不准使用任何流動應用程式將資料從流動裝置上自動上載或同步至其他未獲授權的裝置，例子包括公共雲端儲存服務供應商，以及使用雲端技術的流動供應商所提供的備份方案和分享相片的社交媒體。
- 不要在流動裝置上儲存其他系統（例如電郵、提款卡及網絡登入等）的密碼，亦應停用自動儲存密碼功能。
- 不要廣泛地利用決策局／部門所提供的流動裝置作私人用途。

須要事項：

- 跟從決策局／部門所訂立的保安程序。
- 只下載和安裝決策局／部門批准及提供的應用程式。
- 下載／安裝之前，閱讀流動應用程式的私隱政策以及條款和條件。
- 確保操作系統及已安裝應用程式的保安功能已按強化程序中的要求開啟。
- 安裝最新的病毒及惡意程式的識別碼及定義（當有提供時）。
- 對流動裝置的保安漏洞保持警覺，及根據受影響的系統及版本，按指示安裝相關的修補程式。
- 將已加密的完整數據定期備份至獲授權的電腦或儲存器。若裝置存有敏感資料，則必須跟據現行的政府保安要求保護備份資料。
- 關掉非使用中的無線通訊，例如 Wi-Fi、近距離無線通訊、藍牙及／或紅外線連接。
- 啟用網絡連接通知功能，以便在加入網絡之前獲得用戶的確認。
- 停用自動連接 Wi-Fi 或自動加入的選項，避免自動連接到不可信／假冒的網絡。
- 若無須使用具定位功能的應用程式，關掉流動裝置的定位服務。
- 在連接至公共 Wi-Fi 熱點時，要加倍小心，而且在沒有合適保護下，不要接達政府資料。
- 須建立虛擬私有網絡連線到所屬決策局／部門的政府內部網絡。這樣可確保所有傳送的數據都會受到相應的保安控制。
- 妥善保管所持有的流動裝置。在沒有採取妥善保安措施的情況下，裝置須避免處於無人看管的狀態。
- 啟用超時功能，可在無人看管時鎖定裝置。當處理敏感資料時須留意周遭環境，以減少被偷聽及偷窺的機會。

4.1.2.3 流動應用程式的數據保護

使用流動應用程式時，未授權的接達、數據泄露和異常的數據使用會帶來個人私隱的問題。為了盡量減少這方面的問題，流動應用程式功能的接達，操作或授權應基於「最小權限」和「有需要知道」原則，僅授予必要的權限。此外，用戶或管理員應定期檢查裝置上的私隱設置，並在流動應用程式「選擇拒絕」不需要的數據收集。

- **資料收集**。通常應明確說明資料收集的目的，以及透過該程式所收集、使用或處理的數據。為了保護私隱，用戶應避免通過流動應用程式（例如註冊流動應用程式帳戶）提供過多的個人資料（例如身份證號碼、家居地址、信用卡號碼和簽名等）。

- **資料使用**。如果未按照私隱政策聲明或流動應用程式的條款和條件（例如與其他應用程式或機構共享）中訂明的正確方式使用收集得到的資料，則個人資料會造成數據泄漏的風險。除非用戶事先同意，否則個人資料僅應用於原本資料收集目的或直接相關目的。

- **資料保留**。當用戶卸載流動應用程式時，流動應用程式通常會刪除所收集的資料。為了防止收集到的個人資料傳輸到其他應用程式或機構，與應用程式相關的所有個人資料的保留時間均不超過達致原來目的實際所需時間。

- **資料傳輸**。應將所有與流動應用程式相關的個人資料儲存在流動裝置或指定的儲存伺服器中，並由流動應用程式開發者加密。除非事先獲得用戶同意，否則流動應用程式資料（尤其是個人資料和其他與流動應用程式相關的資料）不得外判、轉移、上傳或儲存在其他後端伺服器、公共雲端儲存和其他平台／地點以及第三方機構。

4.1.3 流動裝置的停止使用

於流動裝置管理最後一個階段，裝置可能因為實體受損、停止支援、再分配給其他人員或決策局／部門等，而需要停止使用。決策局／部門應訂立裝置停用程序，包括安全刪除數據、重設流動裝置至出廠設定，以及棄置，令裝置能在沒有洩泄露數據的情況下重用或棄置。流動裝置用戶及管理員應遵照程序，以妥善保護政府數據和減低資料外泄到未授權人士的機會。

管理員

管理員應跟從以下的良好作業模式：

- 檢查收回裝置的狀況。
- 檢查流動裝置是否曾經處理及／或儲存敏感資料。如有懷疑，則當流動裝置曾經處理及／或儲存敏感資料來處理。
- 於棄置、重用或維修流動裝置前，須完全刪除或銷毀政府數據。若裝置存有敏感資料，管理員須依照政府保安的要求來處理敏感資料。如裝置實體受損，用戶應通知管理員儲存在受損流動裝置中資料的保密級別。
- 設回原廠設定（如有）

流動裝置用戶

用戶應跟從以下的良好作業模式：

- 為決策局／部門進行所需的數據備份。
- 由於管理員未必有權接達裝置內的資料，所以在歸還流動裝置前，要完全清除或銷毀裝置內的資料。有關刪除資料的詳情，請參閱《資訊科技保安指引》及《銷毀及棄置儲存媒體實務指引》內的相關章節。
- 盡早歸還流動裝置。
- 建議用戶從官方網站、流動應用程式商店（例如 Apple 的 App Store、Google Play 或 Microsoft Store）或其他已獲得批准的可信任來源下載軟件和流動應用程式前，先仔細閱讀私隱政策和條款及條件。

4.1.4 保安意識培訓

用戶培訓是加強用戶保安意識的重要一環。政府人員應從流動裝置用戶角度理解保安要求，從而將人為錯誤減至最低。應為流動裝置用戶提供培訓，讓他們對關乎流動裝置的保安威脅、保安要求及保安政策有一定程度的認識。

一般而言，流動裝置用戶的意識培訓應包括：

- 流動裝置內敏感資料的保密級別，以及相應的保安要求。
- 流動裝置使用及停用階段的保安要求。
- 遺失或被盜流動裝置的通報機制。
- 流動裝置保安的最新消息及趨勢。

4.2 流動裝置管理方案

流動裝置管理方案有助於遠程管理使用不同流動平台的流動裝置。 決策局／部門應考慮採用流動裝置管理方案，以簡化支援流動裝置的工作，並使流動裝置有更好的保安控制。

應注意由於流動裝置管理方案軟件主要是為流動電話和平板電腦平台而設計的，因此有關方案大多數無法用於管理安裝了桌上電腦平台的便攜式電腦。決策局／部門應查看方案的最新功能。

4.2.1 流動裝置管理方案的功能

流動管理方案對流動裝置（如流動電話及平板電腦）的政策、庫存、保安及服務各方面提供管理功能。以下列出的一些技術功能只供參考，不應視為強制性要求。選擇流動管理方案時，決策局／部門應按其自身的業務和營運環境，考慮實施安全控制的需求。

- 按所制定的配置設定，來部署及配置流動裝置。
- 遠程接達流動裝置並推送最新的修補程式[2]和配置，以增強裝置的保安控制。
- 流動應用程式的管理，例如安裝及移除。
- 為數據接達提供詳細的審計追蹤。
- 執行保安控制，如在使用無線網絡傳送資料時使用虛擬私人網絡為資料加密。
- 監察異常活動。
- 重覆登入失敗後清除裝置內的數據。
- 當流動裝置遺失或被盜時，遙距清除裝置內的數據。
- 容器化 － 通過實體、虛擬、或應用程式容器，提供一個隔離的環境處理數據（請參閱**附件 B**）。

[2] 用於流動裝置平台的修補程式通常由平台供應商提供。如果流動裝置製造商已特設平台，則可能無法應用由流動裝置平台供應商提供的修補程式，因此可能無法及時修復漏洞。

4.2.2 流動裝置管理方案的良好作業模式

以下列舉一些以流動裝置管理方案作流動裝置保安管理的常見良好作業模式。

- 嚴格執行保安政策

  根據部門資訊科技保安政策及其他相關政策、程序及指引執行技術性措施，透過流動裝置管理方案，可以統一地設定於決策局／部門所提供的流動裝置上。應記錄及定期覆檢已制定的流動裝置管理保安政策。

- 用戶及裝置驗證

  當接達內部資源時，應透過以網絡為基礎的裝置驗證、密碼驗證、以權標為基礎的驗證等不同的方法來驗證用戶及裝置。當裝置閒置一段預定的時間後，應自動上鎖。應開啟遙距上鎖功能，以便在裝置相信已遺失、被盜或置於不安全的地點時，管理員可以為裝置遙距上鎖。

- 安全的數據通訊及儲存

  應以嚴謹的加密方法，例如虛擬私人網絡技術，來保護受管理流動裝置與決策局／部門終端服務間的數據通訊，亦應使用嚴謹的加密方法保護裝置內建記憶儲存器及抽取式儲存媒體內的數據。容器內的數據也應該加密。不允許在流動裝置管理領域之外作複製／貼上和剪下／貼上。應啟動遙距清除功能，以應對流動裝置遭遺失或被盜。裝置應在多次驗證失敗後自動清除裝置內之數據。

- 流動應用程式管理權限

  用戶應注意流動應用程式所要求的權限。當用戶下載或安裝流動應用程式時，程式可能會要求用戶授予權限，接達流動裝置上的資料，例如接達聯絡人，收集到過的地點或到過的網站。一些權限對於應用程式的操作不是絕對必要的。另外，在預設模式下，一些流動應用程式可能會要求授予所有功能（例如相機、聯絡人、位置、麥克風、儲存和電話）的所有權限。此類要求可能會帶來個人資料私隱問題。

以下列出了與應用程式權限相關的一些做法：

- 限制分配給每個應用程式接達資源（例如攝像機、麥克風、位置）的權限，以保障私隱。
- 限制應用程式的同步和共享服務（例如本地裝置同步、遠程同步服務和網站）。
- 如無需要，停用流動應用程式的同步服務。
- 當裝置層面的加密遭受破壞或未啟用時，啟用應用程式層面的加密以防止未經授權的接達。
- 驗證應用程式上的數碼簽署，以確保在裝置上只安裝來自可信任來源的應用程式以及程式源碼並未修改。

- 分發和管理流動應用程式

  - 在流動裝置上啟動遙距清除未經授權或可疑的流動應用程式。
  - 將流動應用程式列入白名單，以確保用戶只使用機構批准的應用程式（包括內部開發或捆綁在流動裝置的流動應用程式）。

- 數據駐留

  - 流動裝置管理方案可以是以雲端平台或機構處所為基礎的。一些資料（例如，流動裝置資訊、位置）將被收集並駐留在流動裝置管理方案。如果資料被認為是敏感的，則應首選機構處所的方案以保護數據。

4.3 指定情景的保安指引

本節集中為政府人員使用流動裝置的不同情景提供保安指引，包括安裝流動保安軟件、流動保安風險評估、處理敏感資料、決策局／部門內部共用流動裝置、流動裝置遺失、被盜或發生其他涉及流動裝置的保安事故。與第 4.1 節的良好作業模式不同，這些情景可能在日常運作中經常發生，也會對流動裝置保安帶來明顯影響，例如不當處理敏感資料、由於共用裝置而導致數據泄露給其他部門，或因裝置遺失、被盜及因程式漏洞而導致流動裝置被攻擊而導致數據外泄。

4.3.1 流動保安軟件功能

流動保安軟件（例如防毒軟件）可在流動裝置上進行保安掃描，以防範有害病毒和惡意活動，並保護流動裝置上的個人資料。軟件可在流動應用程式安裝之前先加以掃描，還可以阻止已安裝的流動應用程式接達其他應用程式。

流動保安軟件的功能包括但不限於：

- 防盜／遙距鎖定（裝置或流動應用程式）
- 阻止濫發短訊／來電
- 權限管理器（跟蹤和管理流動應用程式權限，以保護流動應用程式和裝置）
- 私隱顧問（審查安裝在流動裝置上的應用程式，並確保不會泄露敏感資料）
- Wi-Fi 保安檢查
- 實時掃描
- 防病毒保護
- 惡意軟件檢測
- 反網絡釣魚防護
- 安全的瀏覽模式（例如網絡過濾功能，阻止用戶瀏覽具惡意或釣魚軟件的網站或提醒用戶此事）
- 私隱清理器（穩妥地清除瀏覽記錄）

4.3.2 流動保安風險評估

流動保安風險評估旨在幫助用戶在更新白名單及安裝授權軟件和流動應用程式之前，自我評估流動保安。這可以幫助決策局／部門在安裝授權軟件和流動應用程式之前評估流動裝置的保安風險。

建議各決策局／部門製備一份保安檢查清單供用戶參考。各決策局／部門應根據業務操作及保安考慮因素，清楚地擬定他們的清單。清單應包括但不限於以下內容：

- 授權用戶（例如所有員工、指定的小組／員工或管理員）。
- 流動應用程式所需的權限（例如遵從「最小權限」原則，沒有錯誤配置的權限）。
- 接達、收集和使用流動數據。
- 流動應用程式身份認證（例如雙重認證）。
- 流動應用程式的保安（例如數據加密、已知保安漏洞）。
- 數據保護的保安（例如在傳輸過程中進行加密、不上傳也不傳輸來自流動裝置的數據）。
- 流動應用程式的數據儲存（即與流動應用程式相關的數據僅儲存在流動裝置或指定的數據中心）。
- 可供下載的流動應用程式來源（例如官方網站、供應商的應用程式商店）
- 安全的網絡連接（例如流動裝置停用自動加入連接功能）。
- 通過流動應用程式保安漏洞測試工具檢測（即檢測不到流動應用程式有保安漏洞或惡意行為，因此通過了測試）

4.3.3 處理流動裝置內的敏感資料

為遵守政府的保安要求，決策局／部門須加倍留意政府的保安規定及文件。此外，決策局／部門應採納以下保安作業模式，以保護流動裝置及資料，抵禦常見的保安威脅：

- 不要在流動裝置上處理絕對及最高機密資料。
- 不要在私人擁有的流動裝置上處理機密或限閱資料。
- 在流動裝置上儲存或傳送敏感資料時加密資料。
- 盡量避免於流動裝置上儲存敏感資料。
- 除非資料得到適當保安措施的保護，否則不要在流動裝置上儲存敏感資料。

- 不要將流動裝置內的敏感資料與公共雲端儲存服務、私人擁有的資訊科技設備或其他未獲授權的裝置同步。
- 停止使用流動裝置時，將裝置內的敏感資料徹底刪除或銷毀，並在丟棄或重用裝置前妥善保護管理儲存裝置。
- 不要在私人擁有的流動裝置上儲存敏感資料。
- 若未能看管存儲有敏感資料的流動裝置，就要將裝置放於一個安全的地方。
- 使用屏幕防窺片減少屏幕可視角度。在使用流動裝置時小心調校屏幕位置，避免其他未經授權人士偷窺屏幕上的敏感資料。
- 在可行的情況下，在使用流動裝置及接達敏感資料配置時，設置多重密碼控制。
- 不要擷取有顯示敏感資料的屏幕。
- 不得將敏感資料傳送到公共資訊科技服務設備及供應商備份服務設備上。
- 提醒政府流動裝置用戶在遺失流動裝置、裝置被盜或裝置有損壞時，要立即通知管理員或負責人員。流動裝置用戶要負起保安責任，在任何時間應保護裝置免於被盜、失竊及損壞。

4.3.4 共用流動裝置

應禁止共用政府流動裝置，除非所涉及的人員均獲授權接達裝置內的所有資料。應按照運作需要來決定共同接達的授權，例子包括部門流動裝置接達小組內的資料、流動應用程式開發的測試裝置，及外出或輪班工作如數據中心操作等。若需要共同接達，決策局／部門應確保所有涉及敏感資料的活動都被審計追蹤及被邏輯接達控制軟件所追蹤。

若政府人員因操作需要而共用流動裝置，有關人員應遵守以下良好作業模式：

- 根據「有需要知道」原則來儲存資料。
- 未經授權不可進行任何備份。
- 在使用完畢或轉交其他人員時登出所有應用程式。
- 不要配置或儲存個人電郵帳戶及密碼。

4.3.5 遺失、失竊及保安事故

流動裝置因體積小而容易遺失或被盜。決策局／部門應檢討及修改其保安事故處理程序，為處理裝置遺失或失竊事故作出必要的調整。當發生保安事故，裝置用戶應根據保安事故處理程序立即報告及升級處理。

決策局／部門應考慮以下良好作業模式處理遺失或被盜的流動裝置：

- 撤銷可能被破解的帳戶。
- 在技術上可行的情況下，遙距清除遺失或失竊裝置內的數據。
- 制定、測試及定期覆檢有關遺失或處理失竊流動裝置的程序。
- 如涉及敏感資料時向政府資訊保安事故應變辦事處滙報事故。

4.4 私人擁有的流動裝置的保安指引

在機構內使用私人擁有的流動裝置，其中一個基本的保安問題是擁有權的界定。由於私人擁有的流動裝置只由持有裝置的員工控制，員工可以隨意安裝任何流動應用程式，這樣可能將惡意軟件帶進裝置內。另外，人員可能藉著修改流動裝置的啟動軟件及／或固件，覆蓋供應商的保安控制以得到更多控制權限及使用上的彈性。這些裝置如在沒有適當保護措施的情況下連接政府內部網絡，可能成為保安漏洞，包括外泄保密資料，以及在政府內部網絡傳播惡意軟件，或者成為被惡意軟件控制的攻擊裝置。就以上保安風險，加上遺失裝置所導致數據外泄的風險，在欠缺適當保護下，應禁止於業務上使用私人擁有的流動裝置。

決策局／部門在考慮採用流動裝置方案而涉及私人擁有流動裝置時，應遵照政府保安要求內有關使用私人擁有資訊科技設備的條文。另外，《基準資訊科技保安政策》[S17] 第 20.1.3 節要求，沒有列入任何保密類別的資料也應保護，以防止不慎外泄。

就處理非保密資料，在使用私人擁有流動裝置時，流動裝置管理及流動數據遺失防護是可行的技術方案，以保護流動裝置內的資料免受非授權接達。流動裝置管理著重於管理裝置以及流動應用程式，而流動數據遺失防護則著重於數據控制。決策局／部門宜參照《數據遺失防護實務指引》，就不同情景加入額外考慮以保護流動裝置內的資料。本文第 4.2.1 節已列出一般流動裝置管理方案的保安服務。

4.5 流動裝置的限制及接達級別

決策局／部門應在流動裝置保安政策中就流動裝置科技的使用訂明業務及保安要求，例如決策局／部門宜限制流動裝置的種類（如根據操作系統版本、流動電話品牌／型號等），並要求多層接達級別，如容許政府流動裝置接達較多資源，而讓運行於決策局／部門流動裝置管理客戶軟件的私人擁有流動裝置則接達有限的資源。

決策局／部門應按風險決定那種類型的流動裝置可以授予那種接達級別。在設定流動裝置保安政策時，決策局／部門應考慮以下幾項因素：

- 對政府保安要求的遵行

  除非已根據政府保安要求執行適當的保護，否則不容許業務上使用私人擁有的流動裝置。

- 工作的敏感程度

  部分工作需要接達敏感資料或資源，有些則不然。決策局／部門宜按業務需要為工作設立限制性要求。

- 技術上的限制

  部分情況可能需要指定流動裝置類型或操作系統，例如一些建基於硬件的保安功能又或一些執行某些特定的流動裝置管理客戶軟件的情況。

- 工作地點

  裝置用於決策局／部門直接管轄的環境內，風險比用於其他不同的地點為低。

5. 流動應用程式開發保安

本節適用於參與開發流動應用程式周期的開發人員。對於需要使用和採用流動裝置和相關管理解決方案的用戶和管理員，請參閱第 4 章 -流動裝置保安管理。

5.1 開發流動應用程式的保安考慮

由於現今流動應用程式會用作接達敏感資料和進行重要商業活動，因此亦可能受到不同的威脅。作為良好作業模式，為開發和維護安全的流動應用程式，在開發流動應用程式的不同階段須作出各項保安考慮和採取保安措施（包括技術與管理層面）。

軟件開發的方法正不斷演變，敏捷軟件開發或 DevOps／DevSecOps（結合「開發」、「保安」與「操作」）等利用反覆式開發程序達致持續整合和持續交付的目的，以更快速及／或更安全地建立流動應用程式。這個方法着重持續的溝通、整合、測量和交付，以促進程式開發、測試及質素保證之間各個程序。無論使用何種方法，都應將安全的流動應用程式的設計嵌入到開發周期的每個階段，尤其是早期階段，以盡量減少保安風險並避免因設計缺陷而導致的重覆工作。

為方便找出在流動應用程式開發過程中的潛在保安風險，以下會探討發展周期的一般階段和主要保安考慮：

發展周期	**保安考慮**
要求	在本階段應連同功能要求一併訂定保安要求，並在軟件開發其他階段進一步加入保安因素。
設計	根據要求階段所定的規格設計應用程式架構。
開發	遵從保安編碼良好作業模式開發流動應用程式和進行源碼保安評估。
測試	確認系統功能的效能和準確性。
推出前	進行保安風險評估和保安審計。
維護與支援	通過不斷的測試和適當的保安控制措施維持保安保證。
停止使用	在程式不再符合目標時，停止使用程式。

5.2 流動應用程式開發周期

5.2.1 要求階段

在要求階段應考慮保安因素，以致保安概念可納入整個開發周期。應連同功能要求一併訂定保安要求，並在軟件開發其他階段進一步加入保安因素。如能妥善訂定保安要求，便可於早期階段解決已確定的風險，大大減少後期階段的額外工作和補救工作。在訂定保安要求時應考慮以下各個方面：

- 架構、設計和威脅模型要求

  應制定程序，確保在規劃流動應用程式的架構和設計時已明確處理保安注意事項。每項組件的功能和保安角色均應清晰界定，並涵蓋威脅模型、安全開發和密碼匙管理等項目，例如在實施前採取相關及足夠的保安控制措施保護數據和交易。

- 數據儲存和私隱要求

  開發者應充分了解所處理數據的類型和敏感度，以及是否涉及關鍵交易。敏感數據可能意外地披露予同一裝置上的其他應用程式，數據亦可能在傳遞期間外泄。此外，與其他類型裝置比較，流動裝置較容易遺失或被盜取。開發者應依循有關私隱的法律和規例（例如《個人資料（私隱）條例》），訂定合適的數據儲存和私隱要求。如流動應用程式對私隱有重大影響，應進行私隱影響評估。

- 加密技術的要求

  應採用加密技術保護在流動裝置儲存和處理或在裝置與伺服器之間傳輸的數據。確保流動應用程式按照業界良好作業模式採用加密技術，包括：

  (i) 使用經核實的加密庫。
  (ii) 正確選擇和配置加密函數。
  (iii) 避免重複使用同一組密碼匙作多種用途。
  (iv) 使用安全的隨機數字產生器產生隨機數值。

- 認證和對話管理要求

  應妥善認證和管理用戶帳戶和對話，包括使用隨機產生的接達權標認證客戶端的請求、執行明確的密碼政策，以及在發現過多登錄嘗試時鎖定帳戶等。應用程式狀態變更也應妥善處理，例如在應用程式從後台恢復時需要重新認證。

- 網絡通訊要求

  開發者應確保流動應用程式與遠程服務端點之間所交換資料的機密性和完整性。處理所有應用程式數據時應使用運用已適當設置的傳輸層保安（TLS）規約的加密頻道。在使用 TLS 時，程式必須執行證書確認功能，不應接受任何自簽及／或不可信賴的證書。另外，程式亦應可偵測有否使用未獲授權證書，以防範網絡攻擊（例如中間人攻擊）。

- 環境互動要求

  應考慮以安全的方式使用平台應用程式界面和標準組件，包括應用程式之間的通訊（程序間的通訊）。

- 程式碼質素和建立設置要求

  開發應用程式時應遵從保安編碼作業模式，例如程式應以可信賴的證書簽署。證書應有有效期。續簽後，應審查證書的安全要求（例如密碼算法、密鑰長度），以確保一些常見的保安漏洞不會繼續存在於新簽發的證書中。流動裝置的預設接達權限應降至最低（例如停用相機／麥克風和預設啓用「不追蹤」功能）。

- 抵禦還原工程能力的要求

  如流動應用程式會處理或接達敏感資料，應採取保護措施以增強程式抵禦還原工程的能力。應考慮採取一系列混淆控制措施，如「應用程式隔離」、「阻止動態分析和竄改」、「裝置綁定」和「模擬器偵測」等。

5.2.2 設計階段

設計階段涉及根據要求階段所定的規格設計應用程式架構。建立程式架構後，開發團隊應參照訂定的保安要求，通過識別潛在的遵行要求問題及保安風險審查相關系統設計。這包括為特定類型的數據設計適當的保安控制措施，並結合威脅模型以識別和處理與應用程式有關的風險。

保安審查亦應在設計階段進行，作為一個檢察點，確保已識別所需的保安要求並將之納入系統設計。

5.2.3 開發階段

經常留意保安編碼標準有助改善保安狀況，並減少發生可導致違反保安事件的常見錯誤。在開發階段進行保安評估，還有助確定所需的保安控制措施，並適時向開發者提供有關程式碼安全的意見。此外，應進行源碼保安評估，及早了解程式碼的質素，以便製作統一和優質的流動應用程式。

5.2.4 測試階段

除用戶驗收測試外，系統測試、壓力測試、回歸測試和單元測試均對確認系統功能的效能和準確性大有幫助。由於相關平台和測試環境各有不同，與網上應用系統比較，流動應用程式的測試可能更具挑戰性。開發者應建立全面的測試計劃以設計測試方式，並訂定「什麼」、「何時」及「如何」等測試細節。

5.2.5 推出前階段

在應用程式推出前和作出重大變更後，應進行保安風險評估和保安審計。每次進行保安漏洞修復時均可能需要更新程式碼，因而可能帶來新的保安漏洞。因此，必須持續評估相關風險和影響，以確保流動應用程式安全。

5.2.6 維護與支援階段

應用程式的新增功能或對現有功能的更新都可能為系統帶來變更，因此應制定、記錄、測試和審查保安措施，確保系統得到妥善保護或免被破壞。持續測試對保障安全十分重要，可保護應用程式免受大部分攻擊。應定期審視應用程式，確保有足夠的保障。

5.2.7 停止使用階段

如應用程式不再符合預定目標或有其他應用程式更能達到預期目的，應考慮停止使用程式。停止使用計劃的建議如下：

- 制定通知方案知會所有相關持份者（例如應用程式用戶）
- 從正式運作環境移除應用程式（例如流動應用程式商店）

5.3 保安設計與數據保密

保安設計與數據保密的概念應納入整個應用程式系統設計及開發程序，以保障數據和個別人士的私隱權。開發者應確保已將保安考慮納入為基本架構設計的一部分，並應審視因應潛在保安問題而作的詳細設計，以及決定和制定應對潛在威脅的緩解措施。在訂定私隱要求時，亦應遵從相關法律、規例和條例（例如《個人資料（私隱）條例》）。在系統設計階段，開發者應注意以下良好作業模式，以保障用戶私隱：

通知用戶

- 知會用戶應用程式將收集什麼資料／數據、有關資料將作什麼用途，以及將如何處理該些資料。
- 容許用戶選擇不查閱／使用個人資料。
- 在用戶要求移除應用程式或刪除帳戶時，讓用戶可選擇刪除所有應用程式相關數據及與帳戶相關的資料。
- 在流動應用程式的安裝頁面上向用戶顯示私隱政策聲明，以解釋數據收集、接達和使用的目的，從而增強用戶的信任度。

數據處理

- 盡量減少收集個人資料（特別是敏感個人資料），並將流動裝置功能（例如相機和位置追蹤）的使用權限降至最低。
- 採用嚴謹的加密功能和接達控制措施保障用戶的個人資料，以免在未獲授權的情況下被接達、外泄或使用。避免將個人辨識資料（例如身分證明文件、通訊記錄）或其他敏感資料儲存在用戶裝置上。
- 未經用戶許可，切勿將敏感資料上載或同步傳輸至外部系統或裝置。
- 在完成聲明用途的資料使用後，清除敏感數據（例如地理位置數據）。

5.4 開發流動應用程式的測試

由於流動作業系統、硬件組件和網絡環境各有不同，因此在流動裝置上測試流動應用程式較在個人電腦上測試網上應用系統更具挑戰性。測試流動程式時應考慮以下各個方面：

測試流動應用程式的功能

為了確保流動應用程式能在支援的裝置上正常運作，應進行功能測試，以驗證應用程式的功能規格。此外，亦需考慮進行不同類型的流動應用程式測試：

- 兼容性測試：確保應用程式能在支援的裝置（如配備 iOS 和 Android 等不同流動平台，以及不同屏幕尺寸和作業系統版本的裝置）上正常運作。
- 效能測試：測量應用程式的效能，如回應速度、可接受的用戶負載和程式穩定性等。
- 系統測試：確保流動應用程式能找出並處理可能出現的異常情況，並能從意外終止事故中恢復正常運作。

測試程式碼質素

開發者在流動應用程式開發過程中會使用不同的編程語言和框架，如沒有遵從保安編碼作業模式，應用程式可能會出現常見的漏洞（例如弱點插入、記憶體損毀和跨網址程式編程）。舉例來說，注入式攻擊多數利用流動裝置的跨進程通訊（IPC）界面，以惡意應用程式攻擊在該裝置上運作的另一應用程式。程式的測試，應可發現可能容許不可信賴輸入的進入點，或發現調用已知的危險源碼庫應用程式界面的地方。

為確保流動應用程式的源碼不會因保安漏洞而受到損害，應盡早進行常規源碼掃描，以檢測任何可能對流動裝置構成風險的保安漏洞或缺陷。

流動應用程式的加密技術

加密技術對於保護用戶在流動網絡環境中的數據至關重要，尤其當攻擊者或可實體接達用戶裝置的情形。開發者應採用妥善的加密方法或合適的密碼匙儲存應用程式界面儲存敏感資料。不要使用任何包含已知漏洞的加密算法或規約。採用良好作業模式和保安配置，確保有關加密算法是最新的，並且符合行業標準。切勿使用過時的加密法（例如 DES）或雜湊函數（例如 SHA1）。應妥善處理不當的配置問題，如密碼匙長度不足、硬編碼的密碼匙和不嚴謹的密碼匙產生函數等問題。

流動應用程式的認證

前端客戶及後端伺服器均應整合和進行適當的身分認證，以防止遭受密碼字典攻擊或暴力攻擊。一般而言，屬非敏感性質的應用程式可考慮以用戶名稱／密碼認證；至於屬敏感性質的應用程式，則通常會考慮使用雙重認證（例如短信和權標）。應進行測試，確保前端用戶及後端伺服器均貫徹執行有關認證程序。

應按以下步驟測試應用程式的認證和授權方法：

- 確定應用程式使用的附加認證方法。
- 找出提供關鍵功能的所有端點。
- 驗證已在所有伺服器端點嚴格執行該些附加的認證方法。

測試網絡通訊

流動裝置與伺服器之間的網絡通訊通常在不可信賴的網絡上進行，因此流動應用程式可能會蒙受網絡攻擊（如小包探取法或中間人攻擊）的風險。在處理敏感數據時，應使用加密連接（例如 HTTPS），以確保網絡數據的機密性和完整性。攔截接受測試的應用程式所接收和傳送的網絡通訊，並確保通訊已加密，例如利用數據包分析器收集網絡通訊，並利用網絡規約分析器以人類可讀格式顯示收集所得的通訊。最後，驗證伺服器已按照良好作業模式進行配置。

5.5 開發安全流動應用程式的注意事項

流動應用程式與其他應用系統一樣，有類似的保安考慮和風險，因此一般有關程式開發的良好作業模式亦適用於開發流動應用程式。因應不同的用途、使用模式和流動平台，流動應用程式開發者亦應留意遠端網絡服務、平台整合和流動裝置的不安全性。開發者在建立安全的流動應用程式時應考慮以下各個方面：

- 一般考慮
- 系統／軟件
- 數據
- 網絡管理

5.5.1 一般考慮

- 處理敏感資料時必須緊記安全及提供充分的保護。
- 知會用戶應用程式將接達和上載什麼資料，以及有關資料將作什麼用途。
- 如會收集個人資料，應提供收集個人資料聲明。
- 採取「最小權限」原則，以最小的系統權限及接達權限執行應用程式。
- 按照良好作業模式開發和執行應用程式。
- 設計和提供方法，讓應用程式能進行保安修補程式更新。
- 如流動應用程式會處理關鍵／敏感數據，一旦發現已被越獄或破解根權限，應拒絕執行應用程式或向用戶發出警告。
- 在處理數據前，必須確認所有客戶端提供的數據，並檢查數據是否在預期類型、範圍和長度的範圍內。
- 在程式活動使用大量數據時知會用戶和得到用戶的同意。

5.5.2 系統／軟件

認證和對話管理

- 避免只使用裝置所提供的識別碼（如 UID 或 MAC 地址）識別裝置，而應利用應用程式和裝置特有的識別碼。
- 採用適當的認證機制，並根據流動應用程式風險評估結果，在處理敏感或財務交易時考慮使用雙重認證。
- 避免儲存密碼；完成計算密碼的雜湊後，應立即清除／刪除載有密碼的記憶體位置。
- 充分利用由流動平台所提供的最新保安機制，以保護用戶的憑證。
- 在每個活動／畫面開始時檢查用戶是否已在登入狀態，否則應切換到需登入狀態。
- 在應用程式的對話超時或用戶登出時，清除和刪除所有與用戶數據有關的記憶體和用作數據解密的主密碼匙。

伺服器控制措施

- 評估流動應用程式的後端服務以找出保安漏洞，並確保後端系統執行已強化的配置和安裝最新的保安修補程式。
- 確保後端伺服器已保存足夠的記錄或資料，以作保安事故偵測及應變和進行調查。
- 檢視應用程式的程式碼，以避免在流動應用程式與後端伺服器之間不慎傳送數據。

程式碼混淆／還原工程

- 於應用程式啓動時驗證應用程式的識別碼，以確保程式碼沒有被更改或破壞。
- 如程式碼沒有被編製成機器碼格式以防止還原工程，應盡量使用混淆軟件，以保護源碼和隱藏應用程式資料。
- 對包含敏感數據的應用程式採用抗調試技術（如防止調試程式附加至程式程序）。

使用第三方／開放源碼庫

- 使用可靠及／或官方版本的軟件開發工具（例如軟件開發套裝、軟件庫），以避免在不知情的情況下引入木馬程式或後門程式。
- 留意流動應用程式所使用的第三方框架／應用程式界面的最新發布，以安裝保安修補程式和進行升級。
- 應先確認所有經不可信賴的第三方應用程式往來的數據（如廣告網絡），才在流動應用程式中使用。

5.5.3 數據

數據儲存和保護

- 只收集和披露程式業務用途所需的數據。
- 按數據的敏感度對數據儲存進行分類和採取相應的控制措施，並根據分類處理、儲存和使用數據。
- 基於「最小權限」和「有需要知道」的原則，應將個人資料加密和對其接達控制有所限制。
- 除非已採取適當的保安措施（例如嚴謹的加密），否則不應將應用數據儲存至外置儲存器。
- 將敏感數據儲存或暫存至非揮發性記憶體時，使用適當的算法和密碼匙長度進行加密，並將流動應用程式所需使用的數據減至最少，以保護數據。
- 對應用程式可接收數據的相關區域進行輸入確認和檢查，以防止客戶端程式碼注入或屏幕劫持。
- 在不再需要敏感數據時，清除和刪除記憶體中所有敏感數據。
- 採用沙盒技術隔離應用程式，通過防止其他應用程式與受保護的應用程式進行互動，提高程式的安全性。

網上支付

- 就使用應用程式將會涉及的費用向用戶發出警告並獲取其同意。
- 如涉及付款資源，應推行保安控制措施（如白名單或重新認證），以防止在未經授權或意外的情況下接達有關資源。
- 如需進行網上支付，應使用安全的流動支付服務。使用由官方提供的應用程式界面／範本，並嚴格遵從其執行指引。
- 知會用戶流動裝置必須支援的最低技術規格（例如 TLS），以進行支付服務。
- 在開發設有網上流動支付服務的流動應用程式時遵守特定的數據保安標準（例如《中華人民共和國個人信息保護法》、PCI DSS）。

5.5.4 網絡管理

通訊保安

- 任何敏感數據（例如個人資料或信用卡資料）的傳遞均應使用端對端加密方法（例如 TLS）以作保護。
- 在使用 TLS 時，程式必須執行證書確認功能，不應接受自簽及／或不可信賴的證書。
- 如得悉應以保密超文本傳輸規約（HTTPS）連接，偵測每項要求的連接是否均已使用 HTTPS。

- 啓動應用級虛擬私有網絡（per-app VPN），安全地從任何地方和在任何流動裝置接達內部網絡資源。

5.6 開發 iOS 和 Android 安全流動應用程式的良好作業模式

開發人員還可以參考由個人資料私隱專員公署發布的開發流動應用程式最佳行事方式指引，指引可在個人資料私隱專員公署網站上找到。(https://www.pcpd.org.hk/mobileapps/practice.html)

*** 完 ***

附件 A: 保安強化配置範本

建議用以下流動裝置強化的保安配置作參考。該保安配置宜按決策局／部門的業務需要進行加強及修改。部分配置需要利用額外保安方案來加強，如流動裝置管理或數據遺失防護方案。決策局／部門宜在有需要時，就保安強化諮詢產品供應商或第三方的顧問。

控制[3]	手提電腦	流動電話及平板電腦
密碼		
需要密碼	是	是
需要複雜密碼（如大小寫不一的字母、數字及特殊字符）	是	是
最短密碼長度	8	8
容許輸入失敗次數	5	5
最長密碼使用期	每三個月到六個月	每三個月到六個月
密碼歷史	8	8
裝置閒置時限	最多 5 分鐘	最多 5 分鐘
其他裝置設定		
偵查裝置有否越獄、根權限被破解，或違反軟件版本	是	是
容許安裝來自可靠來源的應用程式	是	是
容許安裝來自不知明來源的應用程式	否	否
容許備份至供應商的雲端服務	否	否
容許備份鑰匙串及鑰匙存庫	否	否
容許分享相片	否	否
容許透過通用串列匯流排傳送檔案	若加密，是[4]	若加密，是 [4]
容許用戶接受不可信傳輸層安全協議證書	否	否
容許修改帳戶設定	否	否

[3] 所列項目均是用於控制流動裝置（包括手提電腦、流動電話及平板電腦）的控制項目範本。項目未必全面詳盡，因此決策局／部門應按業務需要修改成最合適的要求清單

[4] 應加密所有儲存在流動裝置或抽取式媒體內的數據

控制[3]	手提電腦	流動電話及平板電腦
容許網絡共享設定	否	否
容許利用生物特徵為裝置解鎖	否	否
在鎖定畫面顯示訊息	否	否
修改藍牙設定	否	否
容許傳送診斷性數據及使用性數據至流動裝置供應商	否	否
裝置需要加密（例如，全磁碟或檔案為本的加密）	是	是
啟用審計追蹤	是	是
使用自動時間或與可靠時間伺服器同步	是	是
強制加密備份	是	是
啟用遙距清除功能	未能使用 [5]	是
啟用多次登入失敗本機清除功能	未能使用 [5]	是
容許郵件預覽	否	否
容許訊息預覽	否	否
啟用自動連接／自動加入網絡	否	否
啟用詢問是否加入網絡	是（如有）	是（如有）

[5] 手提電腦操作系統未必能提供遙距及本機清除功能，因此決策局／部門宜考慮手提電腦失竊的風險，並採用加密方法作為補償控制

附件 **B:** 容器化技術

流動裝置管理策略的核心目標，是為私人擁有流動裝置內的個人和業務用應用程式及相關數據劃分界線，即現在所稱的容器化，將業務應用程式和相關數據安放於數位容器（實體或虛擬）內，以規管應用程式的行為，並防止應用程式與個人應用程式間有未授權的互動。

不同供應商提供的不同容器可以分為三種類別：實體容器、虛擬容器，及應用程式容器。

實體容器

實體容器於流動裝置晶片組或核心層面將業務應用程式（及其數據）與個人應用程式分隔。實體容器於硬件層面分開流動裝置用戶的業務環境與個人環境。這意味於核心層創建一個個別的操作系統層疊，專門儲存及操作業務應用程式。這操作系統層疊與用戶一般應用程式所使用的操作系統層疊截然不同，亦因此管理員可在這「實體容器」內執行個別機構的安全規定。實體容器其中一個主要保安重點是操作系統層叠一般需要借助個別處理器的處理能力。

實體容器其中一個最大優點是其徹底的保安隔離。由於實體容器將另外的操作系統層疊從正常操作系統層疊隔離，因此完全斷絕業務與個人應用程式間的互動。亦由於這是一個分開的平台，所以不會繼承該流動裝置上的漏洞。

但層疊層面的分隔亦為實體容器方案帶來一個主要缺點中斷了用戶的體驗。每當用戶登入流動裝置的正常操作系統層疊後，都需要登出然後登入另外的操作系統層疊才能使用業務應用程式；而當用戶想用回個人應用程式時，又需要將過程反覆重覆一次。不斷的轉換不但為用戶帶來不便，亦會在一段時間後對用戶生產力造成影響。現時，實體容器方案依賴操作系統支援；第三方及內部軟件開發者需要個別調整應用程式以支援實體容器。

虛擬容器

業務應用程式被分隔儲存在操作系統中的一個加密工作間內，尤如一個執行多個應用程式的沙盒。在虛擬容器內，政策管制應用程式間可以進行甚麼類型的互動。所有容器內應用程式間的互動只能在容器內發生，而所有虛擬容器內應用程式的數據於虛擬沙盒範圍內仍然保持安全。

流動裝置用戶需要輸入另外的密碼來驗證容器以進行業務活動。在使用虛擬容器的情況下，業務應用程式與個人應用程式之間的邏輯分隔由操作系統及核心負責。由於容器於流動裝置內運行，因此裝置操作系統的漏洞可能影響容器的保安。此外，此方案需要第三方及內部軟件開發者個別調整應用程式，以支援個別供應商的容器環境。虛擬容器策略亦需要個別技能及額外的行政工作來持續支援。

應用程式容器

應用程式容器為每個獨立應用程式及相關數據提供一個獨立的安全沙盒，並能讓管理員提供更仔細的控制以保護機構數據，同時給用戶提供無縫的用戶體驗。在此方案下，管理員可以選擇配置適用於所有應用程式的一般政策、個別應用程式的專屬政策，或結合以上兩者。管理員亦能仔細控制每個應用程式的數據流向，例如進入與外出的通訊。另外，由於每個容器內的應用程式數據都是獨立地加密及由政策保護，因此即使流動裝置感染惡意軟件，業務應用程式仍能得到保護。

由於容器是在應用程式上執行，用戶一般無需經常進出容器內外的環境以轉換個人及業務應用程式。無論是個人或業務應用程式，用戶都能夠輕易看見及接達獲准使用的應用程式。混合使用應用程式層面的政策管制及加密，能給決策局／部門更高的保安水平以保持業務應用程式及資料安全。

附件 C: 評估授權流動應用程式的指引

1. 評估流動應用程式的指引

為了評估流動應用程式是否適合安裝，建議各決策局／部門了解流動應用程式是否可以滿足業務或操作需求，以及流動應用程式的保安是否足夠。一個重要的考慮因素是安裝流動應用程式後，不應導致現有流動環境的保安程度受損或導致數據外泄。

建議各決策局／部門採取風險為本模式，循以下各方面評估流動應用程式：

- 流動應用程式的功能
  決策局／部門除了解流動應用程式是否適用於支援業務或操作，還應評估流動應用程式提供的所有功能（包括那些額外功能）是否存在任何風險，這些風險可能會影響流動環境的保安程度。 如果可能的話，請停用不必要的功能。

- 流動應用程式的聲譽和可信度
  現成的流動應用程式必須是在官方流動應用程式商店（如 App Store 或 Google Play）可供下載的。此外，必須從可信任的流動應用程式商店下載以進行安裝。最好能顯示該應用程式有大量下載或獲取安全驗證證書，例如 ISO / IEC 15408，通用標準。

- 沒有惡意軟件
  決策局／部門下載了流動應用程式後，應用流動平台提供的保安工具掃描該應用程式，以檢查是否不含病毒，間諜軟件，惡意軟件等。

- 流動應用程式所需的合理權限
  流動應用程式權限可讓應用程式接達流動裝置的資源（例如聯絡人，訊息，相機，位置，電話，儲存空間等）以及與該流動裝置的其他流動應用程式（例如瀏覽器）進行互動。決策局／部門應檢查授予流動應用程式的權限是否合理。

- 與後端平台的連接
  決策局／部門應評估流動應用程式是否會自動連接到外部後端服務，網站或雲端平台，以了解將要與之作互動的網站或雲端平台是否合宜，是否涉及自動收集數據（例如了解有關徵求用戶同意的披露協議），以及是否涉及任何潛在的敏感資料。

以上準則僅作為一般指引，並非詳盡無遺。建議各決策局／部門定期監察流動應用程式的更新，例如該程式在官方流動應用程式商店是否仍可供下

載。對於更嚴格的保安要求，建議各決策局／部門進行保安風險評估及審計以及流動應用程式源碼掃描，以了解流動應用程式源碼的保安程度，以及第三方工具（軟件庫，廣告網絡，API 等）的適當用法。

2. 更新用於業務的應用程式白名單

關於白名單的訂定，一些決策局／部門可能會採用軟件資產管理來備存軟件清單和軟件特許使用權，以確保決策局／部門使用獲授權的軟件和流動應用程式。軟件資產管理可以幫助決策局／部門控制軟件的採購，減少誤用流動裝置和並非蓄意侵犯版權的風險，並盡量提高用戶的工作效率。軟件資產管理中的獲授權清單可以視為供用戶在決策局／部門的流動裝置安裝獲授權軟件和流動應用程式的白名單。 另外，亦可考慮在決策局／部門流動裝置所預先安裝的流動應用程式清單。這兩個清單應定期作檢討，以確保獲授權軟件和流動應用程式的清單是最新的。

如軟件或流動應用程式不在應用程式白名單中，用戶應提交請求和相關理據（例如支援業務需求／操作，提高工作效率）。建議決策局／部門按 4.3.2 節中所訂明的要求，為流動應用程式進行流動保安風險評估。所有決策局／部門均應遵從所有軟件和流動應用程式的特許使用權，購買協議和知識產權署所建議有關版權的現有法例。建議各決策局／部門仔細閱讀私隱政策以及軟件或流動應用程式的條件和條款。如有疑問，建議各決策局／部門諮詢軟件供應商或知識產權署。各決策局／部門在通過審批機制獲得決策局局長／部門首長的批准後，必須相應地更新應用程式白名單。

3. 白名單和黑名單樣本

白名單列出受信任和獲授權的軟件或流動應用程式，這些軟件被認為是可以安全地安裝在各決策局／部門提供的流動裝置上。在制訂應用程式白名單時，各決策局／部門應參考其備存的軟件資產管理的軟件清單。此外，應定期更新和檢討應用程式白名單。

黑名單與白名單相反，列出禁止在流動裝置上安裝或運行的軟件和流動應用程式，因為可能會導致網絡安全威脅。但要更新黑名單得花費不少工夫。

通常白名單和黑名單應包括以下資料以供參考。

白名單配置（包括政府自行開發／授權的應用程式）

序號	配置設定	樣本值
1.	白名單流動應用程式 – 名稱	GovHK Notifications
2.	白名單流動應用程式 – 開發人員／供應商	HKSARG
3.	白名單流動應用程式 – 版本	2.1.0

4.	平台（例如 iOS, Android, Windows 10）	iOS / Android
5.	裝置（例如 iPhone, iPad, Android phone, Android tablet, laptop）	iPhone/iPad/Android phone/Android tablet
6.	嘗試安裝白名單流動應用程式時要執行的操作	允許接達/ 啟用
7.	授權接達的用戶組（例如所有用戶、指定小組的用戶、高級經理或更高級別）	所有用戶
8.	理據	用於測試不同應用程式上的互用性
9.	軟件類型（例如從網站上免費下載，通過流動應用程式商店免費下載，個人購買的特許使用權）	通過流動應用程式商店免費下載
10.	條款和條件的網頁連結	https://www.xxx.com/licensing.html
11.	批准日期（YYYYMMDD）	20201213
12.	批准的到期日（YYYYMMDD）	20221213
13.	開源軟件（例如 Y、N）	N
14.	免費軟件，共享軟件或已購買	免費軟件

黑名單配置

序號	**配置設定**	**樣本值**
1.	黑名單流動應用程式 – 名稱	MyGame
2.	黑名單流動應用程式 – 開發人員／供應商	GameDeveloper
3.	黑名單流動應用程式 – 版本	1.0.3
4.	平台（例如 iOS, Android, Windows 10）	iOS
5.	裝置（例如 iPhone, iPad, Android phone, Android tablet, laptop）	iPhone/iPad/Android phone/Android tablet
6.	嘗試安裝黑名單流動應用程式時要執行的操作	禁止接達
7	加入黑名單的日期（YYYYMMDD）	20201220