警察通例

第 19 章

資訊及通訊科技設施 18/09

19-04 提供和處置電腦和通訊設施及設備 17/14 11/16

警隊所有資訊及通訊科技設備和設施一律須由資訊系統部或經該部門安排購置、安裝、搬移、維修、改良及處置。人員應按照第三期顧客為本帳戶管理系統訂明的有關程序及工作流程處理。警隊所有資訊及通訊科技設備和設施的保安措施均須符合《政府保安規例》及警隊資訊保安策略。

19-12 警隊資訊及通訊科技設備的保養 17/14 11/16

資訊及通訊科技設備的保管人須負責其轄下設備的儲存、保安、日常會計及檢查。

2. 單位指揮官須確保：

(a) 所有資訊及通訊科技設備及設施使用者均須遵照製造商及資訊應用科／通訊科的操作指示，以及採取有關的預防及安全措施；

(b) 只有曾受訓的警隊人員才可使用需要接受培訓後才可使用的資訊及通訊科技設備和設施；

(c) 對於並非每日使用的警隊通訊設備，須至少每季一次或按照製造商或通訊科的指示進行運作測試及實際檢查，並按照指示處理電池（如設備由電池供電），以免設備損壞或發生故障；以及

(d) 只可由曾受訓的槍械庫人員或獲授權人員為無線電對講機及其他警隊通訊設備裝上或拆除天線、小型話筒設備或配件。

3. 警隊資訊及通訊科技使用者不得干擾或拆除任何警隊資訊及通訊科技設備或配件。只有資訊系統部或獲授權人員方可進行有關保養或維修工作。

02/13
17/14
11/16

19-14　呈報損毀／遺失資訊及通訊科技設備

人員如發現任何資訊及通訊科技設備（包括租用的設備）遺失或損毀，必須按照《警察通例》／《程序手冊》第 14 章所訂明的規定，立即作出報告。負責處理遺失或損毀資訊及通訊科技設備的單位，必須遵照《警察通例》／《程序手冊》第 14 章有關條文處理。如遺失的設備包含警隊資料，更須遵守《程序手冊》第 19 章的條文處理，並須參考載於警察內聯網上的事故應變及管理藍圖。

2. 資訊系統部資訊及通訊網絡管理中心只負責安排撤銷警察流動無線電話服務，並不負責處理重新啟動有關服務或更換遺失的警察流動無線電話。警察流動無線電話如有遺失，須立即向資訊及通訊網絡管理中心報告，以便撤銷服務。如需重新啟動服務或更換電話，使用者單位須透過第三期顧客為本帳戶管理系統向資訊系統部提出申請，以作安排。有關程序同樣適用於處理警隊智能通訊器材的遺失事宜。

3. 《程序手冊》第 14-03 條訂明，在完成調查後，單位指揮官須把「政府物料遺失／損毀報告表格」（Pol. 225 表格）送交資訊系統部〔經辦人：警司（業務服務課）〕。有關所有遺失及無法維修的損毀個案，人員必須按照《程序手冊》第 14-05 條的程序註銷有關設備；如需更換設備，人員可於註銷後在顧客為本帳戶管理系統提交申請。

4. 包含保密或個人資料的資訊及通訊科技儲存設備（例如手提電腦和數據儲存裝置包括軟磁碟、光碟／數碼影像光碟、電子手帳、USB 儲存裝置等）如有遺失，當視作違反保安規定。持有人必須立即向其單位資訊科技保安主任報告，以便他在 24 小時內呈報警務處助理處長（資訊系統）〔經辦人：警司（保安及支援）〕。人員必須按照《程序手冊》第 19-22 及 19-23 條的程序處理。

5. 警隊分發並包含警隊資料的USB手指驅動器如有遺失，必須以高度靈敏的方式嚴肅處理。有關的單位指揮官必須按照《程序手冊》第 19-23 條進行風險評估。有關的風險評估報告須由呈報遺失的時間起計 72 小時內送達警務處助理處長（資訊系統）〔經辦人：警司（保安及支援）〕。

19-15　使用資訊及通訊科技設施及設備的一般規則　09/10 02/13 17/14 11/16

單位指揮官須在警察物料系統備存所有資訊及通訊科技設備的最新記錄，包括持有人的資料，以及其單位所管轄的設備編號／識別號碼。資訊及通訊科技設施的資料如與存貨記錄不符，人員應通知資訊系統部〔經辦人：警司（業務服務課）〕。

2. 單位指揮官必須確保電腦及電訊設備室、警察電話設備室及 999 設施（包括存放有關附屬設備及電池的房間）鎖上，未獲授權人員一律不准進入。這些房間不得用作儲物室或作其他用途。單位指揮官必須確保設備室的鑰匙由有關的值日官妥為保管，或當資訊系統部技術支援小組有需要時，可以在全日任何時間獲准進入有關房間。此外，單位指揮官須至少每月一次根據《警隊資訊保安手冊》附件 E 的核查清單，安排定期檢查有關房間的環境狀況及空調設備的操作情況。如有危險迹象（包括滲水），須立即向機電工程署或建築署報告。單位指揮官須確保填妥的清單妥為存檔，以供查核。如發現任何不當之處，須立即通知資訊系統部資訊及通訊網絡管理中心（電話：2860 3444）。

3. 人員須負責所有由其照管的警隊通訊設備（包括電話卡）發出或接收的收費服務，包括但不限於國際直撥電話、漫遊、短訊服務、多媒體簡訊服務、流動數據服務及其他資訊服務。人員並有責任向政府悉數償還所有與核准公事無關的費用。

4. 利用警察總部通訊中心的警隊國際直撥傳真終端機發送的信息，應先呈交督察或同級人員批核內容及授權發送，方可交給警察總部通訊中心值日官處理。

5. 警察總部通訊中心值日官須確保所有接收的傳真及文件，盡快送交或傳送至適當的人員處理。

6. 除另有訂明外，所有警隊的資訊及通訊科技設備只可用作公事用途。人員須負責妥為保養和使用警隊資訊及通訊科技設備，並須負責因濫用、損毀或遺失由其照管的設備所引致的任何費用。除資訊系統部的人員或獲授權承辦商外，人員不得准許其他人干擾由其照管的設備，或在有關設備附加裝置或進行改裝。

19-16　手提無線電對講機的收發程序　17/14

各槍械庫均須設置巡邏裝備登記冊（Pol. 10A 表格），以記錄每次收發手提無線電對講機的詳情。手提無線電對講機及其配件的保安程度，應與槍械及彈藥相同。

2. 在派發手提無線電對講機給一組人員（例如準備值勤的隊伍）時，須由一名職級不低於警長的人員在場監督。在交還對講機時，亦須由警長在場監督。

3. 警務人員在領取手提無線電對講機時，應在存於槍械庫的 Pol. 10A 表格上簽署，並須小心妥為保管有關設備，直至交回槍械庫簽收或妥善地交給另一名人員為止。

4.　　獲發手提無線電對講機的人員在完成任務後，須立即把對講機交還槍械庫，但隨時候命工作的人員則不在此限。

5.　　槍械庫人員須小心檢查收回的無線電對講機，確保器材未曾受到干擾。

02/13　6.　　如手提無線電對講機報稱遺失或不知所終，應立即通知資訊系統部資訊及通訊網絡管理中心，以便撤銷手提無線電對講機的功能。

17/14
11/16　**19-21　　資訊保安**

資訊保安有賴警隊每一名人員通力合作。為保護和避免警隊資料在未獲授權或意外的情況下被接達、使用、披露、中斷、竄改或破壞，警隊已制定警隊資訊保安策略供所有人員遵守，以確保資料的保密性、完整性和可用性。《警隊資訊保安手冊》載有有關資訊保安的資料、建議及指引。不遵守《警隊資訊保安手冊》的內容，並不一定構成違反指令，但屢次或公然違反有關手冊內容，有關人員將會受到紀律處分。

2.　　為了在資訊及通訊科技的方便與實施資訊保安措施的必要之間取得平衡，警隊每名人員必須遵守《警隊資訊保安手冊》的下列警隊資訊保安政策及其具體指示：

(a)　**取用資料政策**－所有警隊人員只可根據「需要知道」的原則，取用儲存在資訊及通訊科技系統內與其職務有關的資料。警隊會按照「最小權限原則」向使用者授予使用權限。

(b)　**實質保安政策**－放置資訊及通訊科技設備以供儲存或處理資料或電子數據的地點，應避免位於存在盜竊、水害及熱害等風險的地方。如有需要，單位資訊科技保安主任應向機電工程署、建築署或有關的業務服務課人員求助，安排搬移設備。

20/24　(c)　**人事保安政策**－**人事保安政策**－對於工作上可接觸保密或敏感資料或數據的人員，警隊或需就其誠信進行保安審查。使用資訊及通訊科技設備的人員應接受訓練，以減低意外披露或刪除數據的機會。按照《程序手冊》第 70-05 條管限職位調派安排，人員在接達不同警隊資訊及通訊系統或使用警隊資訊及通訊裝備可被施加限制。

02/13　(d)　**硬件及軟件資產管理政策**－應遵照第三期顧客為本帳戶管理系統的工作流程，以處理有關購置、調配、搬移和處置資訊及通訊科技設備和設施的事宜。警察物料系統應盡快更新，以便進行非耗用物料查核工作（《程序手冊》第 14-10 條）和根據《警隊資訊保安手冊》進行檢查。

(e)　**資料分類政策**－資訊及通訊科技系統擁有人或資料發送人須按照《政府保安規例》第三章把檔案／文件、存有保密錄音或視聽記錄的媒體或盛載媒體的保護盒、及抽取式或手提媒體上的數據，適當地分類和加上標記／標籤，以便對資訊及通訊科技系統實施適當的保安措施。

(f) **資料管制政策：**

(i) 所有以電子或硬複本形式儲存的保密資料或數據（例如個人資料）必須視為可能屬敏感資料，並須採取措施以防遺失、被人擅自取用或泄露。人員必須遵守《政府保安規例》所載的保安規定。

(ii) 資訊及通訊科技系統監督必須實施保安措施，以防有人擅自披露經由相關系統處理或儲存的資料和數據。負責處理資料或數據的人員也須履行同樣的責任。

(iii) 須採取保安措施保護敏感或保密資料，例如使用警隊提供的工具進行加密，以及利用密碼保護電子檔案／數據。當個別人員使用獲發的警隊智能通訊器材和抽取式儲存媒體儲存列為「限閱」或以上級別的資料或數據包括個人資料時，均須把資料或數據加密。

(iv) 警隊人員不准使用私人的資訊及通訊科技設備（例如流動裝置、個人電腦、記憶卡、USB 手指驅動器或非政府提供的儲存設施）儲存保密的電子資料或數據。凡批准和使用私人的資訊及通訊科技設備作公事用途，均須符合《警隊資訊保安手冊》的規定。 02/13

(v) 除非事先獲得警司或以上職級的直屬上司批准，否則警隊人員不得把列為「機密」或以上級別的資料或電子數據（儲存在任何媒體內）帶離警察處所。

(vi) 除非有關設施裝有資訊系統部批准的加密設施，否則保密文件不得經電子郵件、傳真或互聯網發送。人員在處理個人資料時，也須按照《警察通例》／《程序手冊》第 76 章訂明的指示辦理。

(g) **網絡保安政策** – 互聯網為全世界交換資訊的公共平台，經互聯網傳送的資料容易被截取或意外地向公眾披露。根據《政府保安規例》及《警隊資訊保安手冊》，人員不得把列為「限閱」或以上級別的警察資料，在沒有加密的情況下經互聯網或其他不可靠的領域傳送。

(h) **遠程接達保安政策** – 警隊人員只准透過正式渠道（例如家居警察內聯網、家居接達警察內聯網）或預先批准的渠道（例如警隊智能通訊器材、由獲授權人員或承辦商遠程保養的安全渠道）接達警隊資訊及通訊科技系統。

(i) **電郵保安政策** – 警察電子郵件網絡（警察電郵網絡）只供警隊人員作公事用途。把警察電郵網絡的電郵地址登記到與公事無關的網站應予避免。警察電郵網絡只准用於警察單位之間及與其他政府部門之間傳送資料，而郵件的內容最高為「限閱」級別。此外，警隊人員可透過警察電郵網絡，以附加檔案形式加密傳送「機密」資料，但使用者須使用警隊提供的數碼證書和加密工具進行加密。人員亦可使用機密電郵系統或機密信息應用系統傳送附有「機密」級別內容的資料，但發信者及收信者雙方均須為政府部門的機密電郵系統或機密信息應用系統用戶。有關規管使用警察電郵網絡的詳情，可參閱《程序手冊》第 19-24 條。警隊人員應警覺，其他非由警隊提供的電郵服務一般並不安全，因此應使用警隊提供的電郵系統（即警察電郵網絡、機密電郵系統、機密信息應用系統或其他專用的通訊連結）傳送敏感或保密資料。

(j) **防毒管理政策** – 警隊資訊及通訊科技系統及設施須由能夠自動更新並具有最新病毒定義的防毒軟件保護。負責管理資訊及通訊科技設備（例如膝上電腦、獨立電腦、使用 Android 作業系統的警隊智能通訊器材等）的警隊人員，如沒有自動更新防毒軟件的支援，應按照資訊系統部公布的指示不時進行手動更新；如在更新時遇有問題，必須向資訊及通訊網絡管理中心求助。

09/10
12/18

(k) **有關使用私人擁有的資訊及通訊科技設備作公事用途的政策：**

(i) 警隊人員如未獲事先批准，不准使用私人電腦或任何形式的數據儲存裝置作公事用途。遇有特別申請，須呈交警務處助理處長（資訊系統）批核。

(ii) 然而，警隊人員可在不涉及保密資料的情況下，使用私人流動電話作形勢掌握用途，惟不准使用私人流動電話蒐集證據或記錄個人資料。

(l) **淨桌政策** – 警隊人員在離開辦公室或辦公桌時，須確保妥善保護以任何形式儲存的敏感或保密資料免被未獲授權讀取，儲存形式包括文件及數據儲存媒體裝置（如軟磁碟、光碟／數碼影像光碟、USB 驅動器、記憶卡等）。

(m) **密碼保安** – 所有資訊及通訊科技使用者均有責任確保其獲發以接達任何警隊電腦、應用程式、電子服務和警隊智能通訊器材的密碼保密。人員不准使用其他使用者的用戶名稱／密碼，亦不得與其他使用者共用其用戶名稱／密碼。單位指揮官及警察流動無線電話或電話卡持有人須確保不會向未獲授權人士泄露機密資料，例如警察流動無線電話或電話卡服務代碼，以及個人密碼。

19-25　保安遵行 – 自我評估及審核　17/14 11/16

資訊系統部保安小組須按照警務處助理處長（資訊系統）的指示，對警隊資訊及通訊科技系統和使用者單位進行資訊及通訊科技系統保安與遵行審核。單位指揮官及人員應協助資訊系統部保安小組人員到達或進入所有警隊資訊及通訊科技設備、設施、有關文件、工作地方、電腦室及數據儲存地方，以便進行審核。

2.　單位指揮官或系統擁有人如欲獲得豁免審核，可以書面形式向警務處助理處長（資訊系統）〔經辦人：高級警司（業務服務科）〕申請，並詳述理由。　02/13