附件 A

投訴警方獨立監察委員會

"警監會"

對於個人資料被泄之報告

二零零六年四月八日

目錄

註：本報告為中文譯本，內容詮釋，以英文文本為準。

1. *發現資料披泄*

1.1 二零零六年三月十日《南華早報》刊載兩篇文章，報道一名電腦使用者利用 Google 搜尋器在互聯網上搜尋商業地址時，發現一個載有警監會檔案號碼及每名投訴人身分證號碼、全名及地址的資料庫。文章亦報道該名電腦使用者已把這宗泄漏資料事件通知廉政公署。

1.2 在上述兩篇文章刊登前，警監會[1]對於可透過互聯網取得上述資料一事並不知情。

1.3 該資料庫在互聯網上出現的經過，當中涉及警監會、EDPS Systems Ltd.["EDPS"]及[redacted]先生["[redacted]先生"]之間的關係。為方便了解，事件發生次序表載於附錄 I。

2. *警監會與 EDPS 之間的合約*

2.1 警監會與 EDPS 之間的合約，分為下列四類：

---

[1] 報告內提及的警監會包括警監會委員會及其秘書處。委員會是非法定組織，主席及委員由香港特別行政區行政長官委任；秘書處職員均爲公務員，負責支援委員會的行政工作。

(a) 開發新電腦統計系統的合約。合約日期為一九九八年十二月二十四日。

(b) 設計監察和核對投訴警察統計資料的電腦程式的合約。合約日期為二零零一年五月四日。

(c) 提升電腦統計系統的合約。首份該類合約由當時的秘書長於一九九九年八月三十日批准，最後一份合約則由當時的秘書長於二零零四年一月九日批准。

(d) 維修保養電腦統計系統的合約。首份該類合約由當時的秘書長於一九九九年十一月二日批准，最後一份合約則由當時的高級助理秘書長(規劃及支援)於二零零五年十月二十七日批准。

2.2 為期一九九八年十二月二十四日的開發新電腦統計系統合約["一九九八年系統合約"]：

(a) 一九九八年八月二十八日，當時的警監會高級助理秘書長(規劃及支援)，就開發警監會新電腦統計系統向承辦商發出報價邀請書擬本，徵詢當時資訊科技署的意見。警監會當時正物色新系統，以便更妥善和快捷地處理所有投訴個案的數據和資料。中選的承辦商將需要把當時資料庫

[FoxBASE+資料庫格式]儲存的舊數據轉換並輸入新資料庫內。

(b) 一九九八年九月二日，當時的資訊科技署建議警監會應向獲邀報價的承辦商提供更多有關電腦系統的背景資料，例如資料量及系統用途，並應參考《物料供應及採購規例》["物料供購規例"]內的適用條款；

(c) 一九九八年九月三十日，警監會透過當時的秘書長發信邀請 EDPS 提交建議書。警監會指出，中選承辦商將需要把原有資料庫所儲存的舊數據轉換並輸入新資料庫。此外，中選承辦商還需要提供持續的維修保養及支援服務。信中並無提及有關資料的保密事宜。

(d) 一九九八年十月十六日，EDPS 提交建議書，建議警監會採用新系統，以 Visual Foxpro 5.0 軟件應用在 Window 95 或更新版本作業系統下運作。EDPS 會向警監會提供數據轉換程式，把舊系統的數據盡量轉換到新系統。

(e) 根據警監會備存的檔案紀要，[redacted]先生與一名當時的警監會助理秘書長於一九九八年十二月十一日會面，該檔案稱[redacted]先生為"Project Manager"

(項目經理)。檔案紀要顯示，當時已詳細告知[redacted]先生有關警監會的背景資料及用戶要求。

(f) 警監會其後於一九九八年十二月二十四日去信EDPS，表示接納其建議。其後簽訂的合約並無明文條款禁止承辦商把有關工作分判。

(g) 該合約的簽訂符合物料供購規例第 280(c)及280(f)條。有關條文載於附錄 II。

2.3 關於二零零一年五月四日簽訂設計電腦程式以監察及核對投訴警方統計資料的合約[" 二零零一年配對程式合約"]:

(a) 二零零一年四月十二日，當時的警監會副秘書長去信 EDPS，邀請該公司就設計電腦程式以監察及核對投訴警察課備存的投訴統計資料提交建議書。投訴警察課及警監會各有一套電腦系統，用以處理投訴警方的統計資料；兩套系統在專用名詞及分類方面有輕微差別。EDPS 獲邀就開發配對系統提交建議書，使兩套統計資料在核對工作時更有效率。二零零一年四月二十日，EDPS 應邀提交建議書。二零零一年五月四日，警監會接納其建議。有關合約的簽訂符合物料供購規例第280(i)條。有關條文載於附錄 III。

(b) 該合約並無明文條款指出 EDPS 在履行合約職責時所處理資料的性質，也沒有明文條款禁止把工作分判。

2.4 有關提升電腦統計系統的合約：

(a) 首份合約由當時的秘書長在一九九九年八月三十日批准。合約規定承辦商為電腦系統提供列印功能，以及為統計系統提供搜尋和列印功能。

(b) 最後一份合約由當時的秘書長在二零零四年一月九日批准[" 二零零四年提升系統合約"]。簽訂這份合約的原因是投訴警察課的電腦系統結構有所改變。因此，警監會電腦系統的數據轉換程式需作修改，以便接收投訴警察課電腦系統所提供的數據。有關合約價值港幣 22,000 元，由一名警監會[redacted]X 女士代表警監會根據物料供購規例第 280(i)條簽訂。合約規定程式修改工作須在二零零四年一月十二日完成，用戶驗收測試須在二零零四年二月十五日完成。該合約並無訂明 EDPS 在履行合約職責時所處理的資料性質，也沒有明文條款禁止把工作分判。

2.5 有關維修保養電腦統計系統的合約：

(a) 首份合約由當時的秘書長在一九九九年十一月二日批准，最後一份合約由當時的高級助理秘書長(計劃及支援)在二零零五年十月二十七日批准。二零零五年十月二十七日的合約["二零零五年維修保養合約"]是警監會與 EDPS 之間唯一依然生效的合約，訂明維修保養期直至二零零六年十月三十一日終止。二零零五年十月二十七日，EDPS 根據合約獲支付有關服務費。

(b) 維修保養合約涵蓋的服務包括修正程式誤差、釐清系統操作、就不正常結果提供意見、熱線電話支援、實地緊急服務及透過電郵更新軟件。

3. ***<u>機密資料外傳至 EDPS / [redacted]先生的經過</u>***

3.1 X 女士在二零零零年一月加入警監會秘書處，職責之一是管理儲存投訴記錄的電腦系統和編製統計報告。

3.2 警監會專責小組[2]已經約晤 X 女士，她並為警監會提供了數份資料。根據 X 女士所言：

---

[2] 警監會於二零零六年三月十一日成立專責小組調查資料被泄事件，成員包括主席[redacted]、[redacted]、[redacted]和[redacted]。

(a) 她曾參與二零零一年配對程式合約、二零零四年提升系統合約和維修保養合約的工作。

(b) 她與[redacted]先生工作交往時，一直以為他是 EDPS 僱員，不知道[redacted]先生是以 EDPS 分判承辦商的身份提供服務。

(c) [redacted]先生從沒要求她提供"模擬資料"以進行 EDPS 答允提供的各項程式測試。程式測試以真實數據進行，而[redacted]先生知道這些數據是警監會的機密資料。她曾向秘書處的高級職員匯報這些測試工作，有關事宜亦記錄在警監會高級職員會議的記錄內。

(d) 她確曾於進行二零零一年配對程式合約和二零零四年提升系統合約期間把一些光碟交給[redacted]先生，並確曾向[redacted]先生清楚說明光碟內儲存了警監會的機密資料。她肯定[redacted]先生完全知道這些資料的性質。

(e) 不過，她並無就交給[redacted]先生的光碟保留記錄，亦無就歸還光碟的事備存記錄。

(f) 她並無接受過電腦科技方面的正規教育或訓練。她信賴 EDPS 和[redacted]先生的專業知識，並且沒有理

由懷疑 EDPS 或[redacted]先生會讓其他互聯網用戶取得這些資料。

(g) 她並無犯錯，不應怪責她。

3.3 警監會在二零零六年四月六日收到 X 女士透過其法律代表呈交的陳述書。X 女士在陳述書內對於指警監會秘書處不應向有關承辦商提供機密資料的說法，表示異議。陳述書內亦表示秘書處須依賴專業承辦商的專業知識、意見和建議。

3.4 專責小組亦在二零零六年三月十一日會見[redacted]先生。他告知專責小組：

(a) 在二零零三年之前，交給他的警監會數據儲存於壓縮磁碟(zip drive)內，他完成工作後把壓縮磁碟交回警監會再用。

(b) 自二零零三年起，載有警監會數據的光碟通常以包裝紙包裹或放入政府信封，供他收取處理。

(c) 他記得最後一次轉換數據的工作在二零零三 / 二零零四年間進行，但不記得確實的日期。

(d) 他知道光碟載有警監會的機密資料，並對自己的疏忽表示歉意。

3.5 二零零六年三月十三日，[redacted]先生透過其律師發信，表示願意向警監會提交一份書面報告。警監會在二零零六年三月二十二日回信接納這項建議，但[redacted]先生的律師在二零零六年三月三十日回覆，表示由於[redacted]先生沒有責任向警監會提供任何資料，警監會應直接向EDPS查詢。

3.6 警監會收到EDPS在二零零六年三月二十二日發出的陳述書。

該公司之立場是：

(a) [redacted]先生從來都不是其公司僱員。

(b) 一九九八年系統合約、二零零一年配對程式合約和二零零四年提升系統合約均沒有禁止分判，亦沒有規定須把分判事宜通知警監會。

(c) 在開發和測試的過程中，已向警監會要求提供測試用的資料。" .....我們並不知道，機密數據會由一名警監會職員抄入光碟後放在警監會接待處，讓我們的工作人員收取。光碟上沒有附上任何保安措施或警告，我們的工作人員無須簽收，亦沒有被要求承諾須審慎處理有關數據。"

(d) " EDPS 從來不知所得的數據屬於機密資料，否則我們定會把有關數據交還警監會，要求提供另一套數據以供測試.....EDPS 沒有'需要知道'這些機密資料。"

(e) " 今次泄漏[資料]的原因，純粹是由於這些機密數據存放於警監會控制以外的地方，並且在承辦商沒有獲得任何警告或通知，以及缺乏必需的管制程序的情況下，被不必要地放進測試環境。"

(f) 他們沒有犯錯，不應被怪責。

4. ***有關資料如何通過 EDPS / [redacted]先生以致公眾可在互聯網上取得***

4.1 [redacted]先生在二零零六年三月十一日會見專責小組時，向專責小組表示：

(a) 他是負責編寫原始程式的人，當時在 EDPS 工作。他其後離開 EDPS。他自二零零二年起以分判承辦商的身分協助維修保養有關程式。

(b) 他把警監會數據放到 China2easy.com[3] 之下的檔案傳送規程(FTP)伺服器的資料夾內，以便在辦公室外進行數據轉換工作。他利用密碼把數據上載到該檔案傳送規程伺服器。他一時疏忽，沒有發覺下載數據是無須使用密碼的。有關資料已上載網上超過兩年。對於這個錯誤，他向警監會致歉。

4.2 [redacted]先生在透過其律師於二零零六年三月十三日發出的信件中承認：

(a) 他確曾把警監會數據存放於伺服器作維修保養/備份用途；以及

(b) 他不再管有任何關於警監會的數據資料。

4.3 二零零六年四月三日，[redacted]先生獲邀就上文涉及他的事宜提出他的意見。他於二零零六年四月四日，透過其律師以書面表示：

(a) 他與專責小組的見面並非"正式會見"，而是屬於"非正式和友好性質，目的在於使警監會可以

---

[3] 有關伺服器由 China Motif Limited 維修保養。有關數據儲存於 China2easy 這個根目錄下的一個子目錄。China2easy 的網址是 http://www.china2easy.com。

知道當時發生了什麼事和傳媒流傳什麼。" 他又聲稱，" 即使準確地引述，亦不可公布當時見面的說話內容" 。

(b) 反對指出[redacted]先生對任何" 疏忽、錯誤" 表示" 歉意、道歉" 。

(c) " 他在當時，即不早於二零零六年三月九日或十一日，才知道光碟載有機密(法例規定須予保護)資料" 。

(d) 進一步聲稱他上載和下載資料均使用用戶名稱和密碼，但 Google 似乎可隨意進入有關伺服器。

[redacted]先生目前的說法與他於二零零六年三月十一日與專責小組見面時的立場截然不同，也與專責小組成員的記憶不符。警監會所得的法律意見認為[redacted]先生沒有法理基礎反對本會披露二零零六年三月十一日他與專責小組會面的內容。

4.4 EDPS 在二零零六年三月二十二日的陳述書內表示，" 在 EDPS 方面，從未發生真實數據被帶到警監會以外地方或讓公眾取得的事。在使用真實數據的製作環境中，從未發生過泄密的事。" EDPS 認為上文第

3.4(d)和第 4.1 段所述並不準確，而且認為這些事宜超出[redacted]先生的專業範圍。其後，EDPS 進一步解釋：

(a) 有關數據理應是測試數據，他們的理解亦如是。

(b) 不存在把“數據上載互聯網”一事。有關網站只是一個連結或接達警監會測試數據檔案的路徑，有關檔案是無意和意外地被存放到有關網站的目錄下。該網站本身並不是提供警監會測試數據檔案的網站，它亦與這些檔案無關。

(c) 有關工程師(大概是指[redacted]先生)使用光碟內的數據建立測試資料檔案時，利用了互聯網的檔案傳送規程(FTP)環境，並設置了用户名稱/密碼保護。任何人士如要在同樣的檔案傳送規程環境下取得檔案，均須提供正確的用户名稱和密碼。當時從未設想過，“互聯網/搜尋器/網站”的環境可以取得有關的資料，但今次意外地出現了這種情況。

4.5 EDPS 再於四月四日透過其律師及於四月五日直接向警監會提交陳述書。這兩份陳述書大部分是重複二零零六年三月二十二日陳述書的內容，表示 EDPS 無人蓄意把警監會資料放到一個互聯網伺服器。有關工程師全部檔案的檔案目錄，包括警監會數據檔案，都是

無意和意外地被放到有關網站的檔案目錄下，因此，該工程師的檔案在不知情的情況下可在互聯網上取得。

4.6 EDPS 在四月五日的信件中解釋，他們已對取得數據的記錄進行分析。根據 FTP 資料庫的分析，EDPS 總結警監會檔案目錄是於二零零四年二月初轉移到有關伺服器。EDPS 認為二零零四年二月至二零零五年九月期間，讀取警監會目錄檔案的次數不多。在二零零五年九月至二零零六年三月期間，數據檔案共被讀取 2016 次。每次都錄得獨一無二並可追查的互聯網供應商地址，可以藉此追查那一部電腦曾經讀取數據檔案。EDPS 分析大部分讀取數據個案所得的資料後，覺得符合其認為大部分用戶並不理解有關資料內容，因而對檢索所得數據不加理會的看法。例外者包括 Google，或許還有另一個互聯網搜尋器，兩者共佔從伺服器取得資料總次數的 64%。EDPS 已把有關資料轉交香港警務處按需要跟進。

4.7 有關各方均已有機會就本報告擬本的相關摘要提出他們的意見，報告定稿前各方面的意見均已獲充份考慮。我們希望把這點記錄在案。

5. ***警監會秘書處一九九八年八月二十日發出的內部通告第33/98號***

5.1 這份通告提醒警監會秘書處人員，警監會秘書處處理的檔案和調查報告性質敏感，因此他們"必須全面保障這些文件/資料的安全，以免未經批准而遭披露。"通告第17段訂明：

> "應盡力確保進入警監會秘書處辦公室的人士不會看到機密文件，除非他們有權查看並確實有'需要知道'....."

5.2 該通告的副本載於附錄IV。雖然該通告明確指示旨在保護"資料"，但其重點主要在於"文件"的保安。

6. ***泄密事件和從中汲取的教訓***

6.1 警監會並無隱瞞導致泄密事件的任何關鍵事實，亦無企圖推卸有關泄密事件的責任。警監會的立場是向公眾全面披露事實，而這正是本報告的目的。警監會已向個人資料私隱專員提供本報告的內容，以便他根據《個人資料(私隱)條例》就事件進行法定調查。警監

會將繼續就個人資料私隱專員的調查給予充分合作，並待調查有結果時加以研究，以及作出相應跟進。

6.2 現時關於導致警監會機密資料外傳至[redacted]先生 / EDPS 的經過，以及為何公眾可從互聯網取得這些資料，X 女士 / 警監會和 EDPS 各執一詞。有關各方亦可能會因此涉及訴訟或紀律程序，警監會實不宜先行作出判斷，亦不宜就有關資料在最初外傳和最終互聯網用戶也可取得兩者之間判定各方應負的責任。

6.3 在不判斷 X 女士就個案提出各點是否屬實，並給予其陳述最大體諒的前提下,我們作出如下建議：

(a) 警監會日後與資訊科技承辦商簽訂的合約，如涉及需進行數據測試，應盡可能不使用機密資料，應使用模擬資料。

(b) 警監會日後與資訊科技承辦商簽訂的所有合約均應訂明，承辦商只可按"需要知道"的準則取得資料，並訂明承辦商履行合約時可能取得的資料屬於機密性質。合約也應訂明承辦商有責任遵守保密規定。

(c) 秘書處應就承辦商收取的機密資料編製記錄，並確保這些資料得到妥善處理及保護。只有在極為

例外並符合保障資料原則的情況下，才可把資料帶離警監會。

(d) 政府應調查涉及事件的公務員有否行為失當。

(e) 檢討通告第 33/98 號，以應付資訊科技日益普及所帶來的風險。

(f) 警監會秘書處職員使用資訊科技處理個人資料時，應提高保護資料的意識。

6.4 在不判斷 EDPS 就個案提出各點是否屬實，並給予其陳述最大體諒的前提下,我們的意見如下：

(a) EDPS 一直向警監會隱瞞該公司和[redacted]先生的真正關係。[redacted]先生的名片載於附錄 V，從中可見[redacted]先生的職銜為 EDPS" Project Manager"（項目經理)。這點與 EDPS 指[redacted]先生只是按資訊科技界所謂"外判"做法聘用的第三方承辦商及從來不是 EDPS 僱員的說法，截然不同。

(b) 與警監會合作的承辦商竟然指稱在履行合約責任時，不知道所用資料的性質，實在不能接受。

(c) EDPS /[redacted]先生是導致公眾可取得有關資料的直接近因。

(d) 警監會在徵詢法律意見後，應考慮是否繼續使用EDPS根據兩方唯一尚未完結的合約中(即二零零五年維修保養合約)所提供的服務，及就法律意見採取進一步行動。

7. *補救措施*

7.1 *向受影響人士道歉*

(a) 警監會於二零零六年三月十一日和三月十七日已通過主席向公眾衷誠道歉。

(b) 警監會將根據目前已收集的資料向每名受泄密事件影響的人士發出書面道歉。

(c) 警監會並會在本港讀者眾多的兩份中文和兩份英文報章刊登道歉信（有關措詞載於附錄VI），向受影響的人士致歉。

(d) 警監會正與保安局局長商討，向受影響的警務人員作出適當的道歉。

7.2 *個人資料(私隱)條例(第 486 章)*

(a) 《個人資料(私隱)條例》第 66 條訂明，任何個人如因該條文說明的違反事項而蒙受損害，則該名個人有權就該損害向有關的資料使用者申索賠償。該條例第 66(2)條訂明有關損害可以是或可包括對感情的傷害。

(b) 警監會將基於每宗個案的情況考慮任何索償申請，並向政府作出建議。

7.3 ***監察以防資料被濫用***

(a) 警監會建議秘書處與進行網上巡邏的警方緊密合作，並與私隱專員公署緊密合作，防止資料遭濫用。私隱專員公署將聯絡各互聯網服務供應商，請他們提示客戶須尊重他人的個人資料私隱權。

(b) 警監會亦已向保安局局長建議實施多方面的信貸監察措施，防止有人利用有關資料謀取利益而使資料當事人蒙受損害。

8. ***其他行動***

8.1 警監會已接納專責小組就泄密一事所提出以下一系列的措施。

8.2 警監會已聯絡本港及海外的主要互聯網服務供應商，要求他們刪除與曝光清單有關的資料，包括清理和整理快取記憶體。

8.3 警監會將與投訴警察課商討採用相同的軟件，避免在讀取有關數據時需進行數據轉換工作。

8.4 投訴警察課所提供的資料光碟，現已存放在一名高級助理秘書長辦公室內的檔案櫃。

8.5 處理資料的電腦現已存放在一個獨立的房間內，而非放在總務室，而且並無連接互聯網。

8.6 只限秘書長或獲其明確許可的人士才可接觸警監會的資料庫。有關電腦現已附設記錄簿，任何人士如欲使用該資料庫，須在記錄簿上簽名，並填寫職銜、接觸資料庫的日期、開始和結束時間。

8.7 第三者應基於'需要知道' 的準則才可取得資料，並且在批准取得資料前，應訂立保安規定，例如令取得資料者表明知道所得資料須予保密、並制定不得使用或披露資料的書面協議。第三者獲取資料時，必須有一名警監會職員在場，並記錄他全部取得的資料。

8.8 現正檢討和重新擬寫通告第 33/98 號，並諮詢政府資訊科技總監辦公室及個人資料私隱專員公署，以期清

楚訂立與《個人資料(私隱)條例》的條文相符的資訊科技保安基準政策。

9. ***貫徹執行職責***

9.1 警監會的職權範圍如下：

(a) 監察警方處理市民投訴的方法，並於適當時進行覆檢；

(b) 定期檢討導致市民投訴警務人員的各類行為的統計數字；

(c) 在警方工作程序中找出引起或可能引起投訴的不當之處；以及

(d) 適當時，向警務處處長，或在有需要時向行政長官提出建議。

9.2 警監會將貫徹執行以上的職責，竭盡所能為市民服務。

二零零六年四月八日　　投訴警方獨立監察委員會

附錄 I

事件發生次序表

1998 年 8 月 20 日	警監會發出內部通告第 33/98 號(附錄 IV)。
1998 年 12 月 24 日	警監會與 EDPS 就開發新電腦統計系統簽訂一九九八年系統合約。
1999 年 8 月 30 日	警監會與 EDPS 簽訂首份提升電腦統計系統合約。
1999 年 11 月 2 日	警監會與 EDPS 簽訂首份維修保養合約。
2000 年 1 月 3 日	X 女士加入警監會秘書處。
2001 年 5 月 4 日	警監會與 EDPS 簽訂設計電腦程式以監察及核對投訴警方統計資料的合約，合約日期為二零零一年五月四日。
2004 年 1 月 9 日	警監會與 EDPS 簽訂最後一份提升系統合約。
2005 年 10 月 27 日	警監會與 EDPS 簽訂最後一份維修保養合約。
2006 年 3 月 10 日	《南華早報》刊登文章導致發現泄漏資料一事。

STORES AND PROCUREMENT REGULATIONS

280. (a) Departments should follow the provisions set out in (b) - (f) below in the procurement of services with a value not exceeding the financial limits stated in SPR 220(a) and consultancy services with a value not exceeding $500,000, which cannot be undertaken by Government departments or for which a Government contract does not exist.

(b) For procuring services with a value not exceeding $20,000, departments must approach more than one contractor for quotations and accept the lowest offer to specification. A department may accept a higher offer provided that the Controlling Officer or an officer specially delegated by him to order the service considers that the rates quoted are reasonable, and certifies this on file.

(c) For procuring services with a value exceeding $20,000 but not exceeding $1,000,000 in respect of construction and engineering works and $500,000 in respect of consultancy and other services, departments must obtain written quotations from not less than five contractors and accept the lowest offer to specification. Departments should designate officers of not lower than the rank of Executive Officer II/Assistant Supplies Officer or equivalent to handle the selection of contractors and to contact them for written quotations, and to record on file the particulars such as the names of the contractors contacted and the reasons for their selection.

(d) In cases where it is not possible to identify a sufficient number of contractors to obtain the minimum number of quotations required, an officer of not less than two ranks higher than an Executive Officer II/Assistant Supplies Officer or equivalent should approve the issue of invitations to contractors. The officer will then make a brief explanatory note on file for record purposes.

(e) Where written quotations are invited, departments should ask contractors to return the quotations in sealed envelopes by a specified time. A quotation opening team comprising two members, with the team leader at a rank not lower than that of Executive Officer II/Assistant Supplies Officer or equivalent, will open the envelopes, date-stamp and initial the quotations.

(f) In cases where a higher offer is to be accepted or less than the minimum number of quotations are received, the officer accepting the selected offer must be of a rank of D2 or above.

STORES AND PROCUREMENT REGULATIONS

280. (i) In cases where a higher offer is to be accepted or less than five written quotations are received, officers at the following levels should approve the acceptance of the offer —

	Value of the Purchase	Approving Officer (not lower than the rank of)
(i)	not exceeding 20% of the financial limits set out in	
	SPR 220(a)(ii)	Senior Engineer or equivalent
	SPR 220(a)(iii) and 222	Senior Supplies Officer/Senior Executive Officer or equivalent
(ii)	not exceeding 50% of the financial limits set out in	
	SPR 220(a)(ii)	Chief Engineer or equivalent
	SPR 220(a)(iii) and 222	Chief Supplies Officer/Chief Executive Officer or equivalent
(iii)	up to the financial limits set out in	
	SPR 220(a)(ii)	Government Engineer or equivalent
	SPR 220(a)(iii) and 222	D1 or equivalent

Ref : (95) in IPCC/CR/3/515/87

Independent Police
Complaints Council

20 August 1998

IPCC Secretariat Internal Circular No. 33/98

Departmental Security Instructions

In view of the large number of CAPO case files and investigation reports, which are generally of a sensitive nature, handled by the IPCC Secretariat, it is imperative that the security of these documents/information should be duly protected to guard against unauthorised disclosure. This circular sets out for information and compliance the security arrangements for the IPCC Secretariat, and the procedures to be followed by staff who are required to handle classified documents. For the purpose of this circular, the word "classified" is used to describe information which is graded Restricted and Confidential, as the bulk of documents handled by the IPCC Secretariat are of a Restricted or Confidential nature. In the event that Secret or Top Secret documents need to be handled, the relevant provisions in the Security Regulations are to be observed.

Personal Responsibility

2. It is an offence under the Official Secrets Ordinance for a Government servant to fail to take reasonable care of, or to conduct himself so as to endanger the security of any document or information, classified or unclassified, entrusted to his care.

3. All officers should take reasonable care to safeguard at all times the security of the office and any office property and documents in their care. They are advised not to leave their personal belongings unattended even during office hours. As far as possible, personal belongings should be locked in the pedestals.

Opening and Closing of the Office

4. The Office Assistants are assigned to perform, among others, the following duties :-

a) To open the office doors at 0800 hrs. and to lock them up at 1830 hrs during weekdays, and at 0830 hrs and 1230 hrs respectively on Saturdays, or earlier/later as necessary;

b) To open the roller shutters at 0845 hrs and to close them at 1715 hrs during weekdays, and at 0900 hrs and 1200 hrs respectively on Saturdays, or earlier/later as necessary;

c) to perform reception duties at the Reception Counter and to answer simple enquiries; and

d) before locking up the office doors, to inspect the whole office to ensure that the exit doors have been locked, all lights and electrical appliances (except for refrigerators, servers and facsimile machines) have been switched off, and all filing cabinets or rooms have been locked.

Departmental Security Officer

5. Senior Assistant Secretary (Planning and Support) (Tel : 2862 8208) is designated as the Departmental Security Officer to assist Secretary/IPCC in overseeing the security arrangements for the protection of personnel, properties, documents and information, in particular the classified documents and information, kept by the IPCC Secretariat.

Incoming Classified Documents

6. Other than personal documents addressed by name in an officer's private capacity which will be handed directly to the addressees, all incoming classified document/letters will be opened and inserted on relevant files as quickly as possible by the Clerical Officer or Personal Secretary II for transmission to the subject officers concerned for action/information. All incoming classified documents must be date-stamped on receipt.

7. When a document classified Confidential or above is received, the Clerical Officer or Personal Secretary II will examine the envelope and check that the seals are intact before the receipt is signed. If there are any signs that the envelope has been tampered with, he or she must report at once to the Executive Officer (Administration), who will inform the Departmental Security Officer for his further action/instruction.

8. Personal Secretary II will maintain a register recording the receipt of all documents classified Confidential and above, the subject matters, date and office of origin, and reference numbers of the subject files. She will also maintain an up-to-date record of the whereabouts of all files which contain documents classified Confidential and above.

Regrading of Documents

9. On receipt of an incoming document, the subject officer(s) should scrutinise its contents to assess whether the classification is appropriate. If necessary, the subject officer(s) will upgrade or downgrade the classification. In case of doubt, they should consult their supervisors.

10. When regrading a document, the old classification must be deleted in ink and the new one marked on the document. The amendment must be signed and dated by the responsible officer.

11. Conversely, with the passage of time, information may cease to warrant a high classification. The responsible officers should downgrade the related files/documents to avoid over-classification. If it is intended that information will be classified only for a short period of time, the 'Temporary' classification should be used.

Transmission of Classified Documents within the IPCC Secretariat

12. Restricted documents are despatched by the Office Assistants while Confidential documents may only be despatched by the Personal Secretary II, the Clerical Officer/respective Assistant Clerical Officer and the subject officers concerned.

Outgoing Classified Documents

13. All classified documents will be typed by Personal Secretary II or Clerical Assistants, as appropriate. The Personal Secretary II or Clerical Officer/Assistant Clerical Officers will seal the envelopes in accordance with Security Regulations 213 and arrange for the despatch of such correspondence.

14. Restricted documents can be sent by fax if the sender notifies the receiver beforehand and ensures that the documents are not diverted on the way. For Confidential documents, transmission by fax must be made through a special equipment (encryption equipment). However, as the IPCC Secretariat does not have such an equipment, government R & D service or personal delivery should be used.

15. Any officer delivering a document classified Confidential or above must obtain a signed receipt from the recipient.

Safe Keeping of Classified Documents

16. Prior to leaving the office, all officers should check that classified documents in their care are properly stored. They should also comply with the following :-

a) confidential documents must be kept in a steel filing cabinet fitted with a locking bar and padlock;

b) restricted documents must be kept either in a locked steel filing cabinet, or in an office which is locked up after office hours and to which members of the public do not have access; and

c) classified documents and the keys to cabinets in which classified documents are kept must NOT be left in pedestals, even if the pedestals are locked.

17. Every effort should be made to ensure that persons entering the office of the IPCC Secretariat will not be allowed sight of classified documents unless they are entitled to see them and have a definite "need to know". Particular care should be taken when messengers, cleaners etc. enter the office.

18. All materials used in the production of a confidential document, from which the contents of such document could be obtained must receive the same degree of protection as the document itself. Examples are shorthand books, carbon paper, typewriter ribbons, floppy disks, etc. Officers concerned should dispose of them in a proper manner and arrange for them to be shredded or stored under secure conditions as appropriate.

19. Where classified correspondence is typed using the computer or with the aid of memory function of an electronic typewriter, Personal Secretary II or Clerical Assistants should arrange to clear the correspondence from the memory of the machines as soon as possible, or keep the floppy disks in a proper place.

Security Inspection

20. The Departmental Security Officer will check the confidential files at least once every six months on the first working day in January and July each year. Records of the results of these inspections should be maintained

Taking Documents Out of the Office

21. Staff are advised not to take classified documents home since it involves the risk that the documents may be mislaid or lost. Where an officer is required to take classified documents home, he should consult the Departmental Security Officer.

Copying of Classified Documents

22. Officers handling classified documents are reminded that copying of classified documents should be kept to the minimum.

23. If an officer wishes to reproduce a document classified Confidential and above, he should approach the Clerical Officer or Personal Secretary II for assistance. A register will be maintained near the photocopier giving details of the reproduction of such documents. The original document will also be endorsed with the number of copies made and the signature of the authorising officer. The Departmental Security Officer will inspect the register during the regular security inspection.

24. Reproduced copies of classified documents must be clearly stamped top and bottom with the appropriate classification.

Destruction

25. To make good use of the paper shredder for destruction of classified waste material suitable for shredding, such waste material should be handed to the Executive Officer (Administration) for disposal, as and when necessary.

Security keys

26. Keys to the various key locks used for the protection of documents classified Confidential and above must be safeguarded at all times. They must not be left in the lock where an unauthorised person might have access to them. Officers are personally responsible for the safe custody of such keys and must take all necessary precaution to prevent them from being stolen or copied.

27. If any key is lost or stolen, this must be reported immediately to the Executive Officer (Administration) who will arrange for the replacement of the lock and advise the Departmental Security Officer for his further action. Keys must not be marked or labelled in such a way that they can be identified, as this increases the risk of the thief or finder making use of the key before the theft is discovered.

28. Any enquiries arising from this circular should be addressed to the Departmental Security Officer in the first instance.

29. This circular will be re-circulated to you every other six months.

( )
Secretary,
Independent Police Complaints Council

Circulation

All IPCC Secretariat staff

c.c. IPCC5/13 (III)

Fax

edps systems ltd. 2370

[redacted]

Project Manager

[redacted]

IAL BUILDING,
WANCHAI ROAD, WANCHAI,
HONG KONG.

TEL 2833·
FAX 2833·
Mobile: 9043·

附錄 VI

投訴警方獨立監察委員會(警監會)向因互聯網上泄漏警監會資料一事以致個人資料遭披露的人士的公開致歉

警監會對閣下資料被泄一事深表抱歉。

就此事因警監會對閣下引起的不便，警監會謹向閣下致以誠懇和衷心的歉意。

警監會現正密切監察情況，並會採取合理措施，以防閣下的資料被濫用。

投訴警方獨立監察委員會

二零零六年四月十日

附件 B

Ref. : (24) in IPCC 5/13 III

Independent Police Complaints Council

21 September 1998

IPCC Secretariat Internal Circular No. 37/98

Handling of Classified Documents

It was agreed at the IPCC Secretariat Staff Meetings that office security and the security of graded document on despatch/delivery were most important. In this connection, your attention is drawn to the following Security Regulations :-

Handling of Classified Documents

Personal Responsibility

SR 190. It is an offence under the Official Secrets Acts for a Government servant to fail to take reasonable care of, or to conduct himself so as to endanger the security of any document or information, classified or unclassified, entrusted to his care.

Safe Keeping

SR 196. CONFIDENTIAL Documents must be kept in a steel cabinet fitted with a locking bar and padlock.

197 RESTRICTED Documents must be kept either :-

(a) in a locked steel filing cabinet, or

(b) in an office which is locked up after office hours and to which members of the public do not have access.

(* It is considered more desirable to keep restricted documents in a locked steel filing cabinet.)

SR 198. Shorthand notebooks, carbon papers, typewriter ribbons, stencils, cylinders, disks, tapes, cartridges, wires and films, and all other materials used to record classified material, must be treated as classified documents.

199. Advice on storage of classified material of other than Hong Kong origin may be obtained from the Government Security Officer.

2. I should be grateful if you would observe the above regulations.

3. This circular will be re-circulated to you every other six months.

for Secretary
Independent Police Complaints Council

Circulation

All Staff

c.c. S/IPCC
IPCC/CR/3/515/87