立法會
Legislative Council

立法會CB(1)2311/07-08號文件
(此份會議紀要業經政府當局審閱)

檔　號：CB1/PL/ITB/1

資訊科技及廣播事務委員會
特別會議紀要

日　期　：**2008年5月30日(星期五)**
時　間　：**上午8時30分**
地　點　：**立法會會議廳**

出席委員　：鄭經翰議員, JP (主席)
李國寶議員, 大紫荊勳賢, GBS, JP
李華明議員, JP
呂明華議員, SBS, JP
陳智思議員, GBS, JP
楊孝華議員, SBS, JP
劉慧卿議員, JP

其他出席議員：涂謹申議員
劉江華議員, JP
余若薇議員, SC, JP
王國興議員, MH
郭家麒議員

缺席委員　：單仲偕議員, SBS, JP (副主席)
黃宜弘議員, GBS
曾鈺成議員, GBS, JP
霍震霆議員, GBS, JP
陳偉業議員
湯家驊議員, SC

出席公職人員：公務員事務局副秘書長3
李美美女士

食物及衞生局首席助理秘書長(衞生)
盧潔瑋小姐

政府資訊科技總監辦公室
政府資訊科技總監
葛輝先生

政府資訊科技總監辦公室
助理政府資訊科技總監(基礎設施及資訊保安)
王錫泉先生

衞生署助理署長(特別衞生事務)
鄺國威醫生

入境事務處助理處長(資訊系統)
關陳雪梅女士

香港警務處監管處處長
杜偉義先生

香港警務處助理處長(支援)
顧履勤先生

應邀出席者 ：<u>醫院管理局</u>

財務總監
謝秀玲女士

質素及安全總監
梁栢賢醫生

醫療信息總監
張毅翔醫生

署理總行政經理(病人安全及風險管理)
李夏茵醫生

<u>香港個人資料私隱專員公署</u>

個人資料私隱專員
吳斌先生, JP

首席律師
郭美玲女士

律師
趙世芳女士

列席秘書 ：總議會秘書(1)3
余天寶女士

列席職員 ：高級議會秘書(1)3
林映儀女士

議會事務助理(1)6
梁美琼女士

經辦人／部門

I. 有關近期遺失可攜電子儲存裝置當中載有由政府部門／公營醫院持有的個人資料及網上洩露由入境事務處持有的機密資料的事宜

(立法會CB(1)1679/07-08(01)號文件 ——	政府當局提供的文件
立法會CB(1)1679/07-08(02)號文件 ——	醫院管理局提供的文件
立法會CB(1)1679/07-08(03)號文件 (只備中文本) ——	2008年5月21日立法會會議的議事錄草擬本，第4項由余若薇議員就"保護個人資料"提出的口頭質詢
立法會CB(1)1679/07-08(04)號文件 ——	2008年5月21日立法會會議，第15項由劉慧卿議員就"檢討《個人資料(私隱)條例》"提出的書面質詢及政府當局的回覆
立法會CB(1)1679/07-08(05)號文件 ——	2008年5月21日立法會會議，第19項由張學明議員就"遺失儲存於電子器材的病人資料"提出的書面質詢及政府當局的回覆

經辦人／部門

立法會CB(1)1692/07-08(01)號文件 ——	2008年5月28日立法會會議，第1項由曾鈺成議員就"政府部門和公營機構對個人資料的保障"提出的口頭質詢及政府當局的回覆
立法會CB(1)1679/07-08(06)號文件 (只備英文本) ——	單仲偕議員2008年5月7日的函件
立法會CB(1)1692/07-08(02)號文件 ——	2008年5月27日的相關剪報
立法會CB(1)1704/07-08(01)號文件 (只備中文本) ——	2008年5月28日的相關剪報
立法會CB(1)1741/07-08(01)號文件 *(於會議席上提交，其後於2008年6月2日發出)* ——	政府資訊科技總監的發言稿)

主席致歡迎辭

主席歡迎個人資料私隱專員(下稱"私隱專員")及政府當局和醫院管理局(下稱"醫管局")的代表出席會議。他隨後邀請政府資訊科技總監辦公室、醫管局及近期發生資料外洩事故的有關政策局和部門的代表，向委員簡述該等事故的背景及已採取的改善措施。

政府當局、醫院管理局及個人資料私隱專員公署作簡報

政府資訊科技總監辦公室

2. 政府資訊科技總監對近期的資料外洩事故表示極度遺憾，並希望藉此機會向公眾致歉。他告知委員，當局剛獲悉一名食物環境衞生署(下稱"食環署")員工向投訴人發出電郵時，竟疏忽地夾附一份載有170名食環署員工病假紀錄的檔案。他隨後簡報各宗個案，包括公務員事務局、衞生署及醫管局遺失或被盜去載有可識別身份的個人資料的便攜式電子儲存裝置，以及網上洩露由入境事務處(下稱"入境處")和香港警務處(下稱"警務處")持有的機密資料。這些個案已全部向私隱專員報告。調查至今未有發現部門核心系統或通訊網絡曾遭破壞。在

所有個案中(入境處的個案除外，因主要涉及旅客資料而聯絡資料不詳)，當局已通知其個人資料外洩的資料當事人，並建議他們格外小心，以免他們的資料可能被濫用。政府資訊科技總監表示，許多資料外洩事故的起因，都是員工對保安規例缺乏認知、不知道須遵從該等規例，以及不大理解個人資料外洩的風險。發生事故後，有關政策局和部門已採取步驟收緊相關的保安程序，提醒員工各項保安要求。員工亦獲提供電腦軟件及硬件，以便在穩妥的環境下工作。政府資訊科技總監接着概述政府資訊科技總監辦公室及各政策局和部門已採取的措施和將會推行的強化計劃，以減低資料進一步外洩的風險，並處理所發現的人為及管理問題。詳細資料載於政府當局的文件(立法會CB(1)1679/07-08(01)號文件)。

醫院管理局

3. 醫管局財務總監就病人資料外洩致歉，並向委員簡述醫管局現行有關保護資料的政策及指引、醫管局資訊科技系統的保安及防止擅用措施、公布指引及員工培訓，以及為加強保護病人資料而採取的改善措施，詳細資料載於立法會CB(1)1679/07-08(02)號文件。

4. 醫管局財務總監表示，醫管局已成立病人資料安全及私隱專責小組(下稱"專責小組")，檢討現時保護病人資料的政策和保安制度，並提出改善措施。專責小組將於3個月內完成檢討，向醫管局行政總裁提交報告。

入境事務處

5. 入境處助理處長(資訊系統)向委員簡述近期的網上洩露資料事故，並特別說明以下各點：

(a) 關於一名新入職的入境事務主任把一些載有可識別身份的個人資料的檔案，複製到他的家庭電腦，導致資料外洩，初步調查已完成，亦已向私隱專員報告該事故；

(b) 該處的應用系統設計並不提供USB接駁功能。所有文件及個人資料都不能下載或放上互聯網。員工是留在辦公室超時工作，而不可把工作帶回家；

(c) 該處已立即採取行動，從有關員工的家庭電腦移除相關的檔案文件及檔案共享應用軟件，並重新把電腦硬碟格式化。該處亦檢查部門內的

電腦終端機，確保沒有安裝未獲授權下載的軟件；及

(d) 發生事故後，該處立即口頭提醒所有員工，並傳閱有關保護資料和正確處理個人資料的保安指引及規例。該處會繼續加強所有員工對這方面的警覺性。

衞生署

6. 衞生署助理署長(特別衞生事務)向委員簡述有關事故及衞生署採取的跟進行動，內容如下：

(a) 警方和私隱專員分別於2008年4月22日及25日接獲報告，指屯門兒童體能智力測驗中心一名醫生遺失一枚便攜式USB閃存盤。該裝置儲存了工作檔案及668名病人的個人資料。衞生署於2008年4月24日以書面通知受影響的兒童及其家人，並建議他們對有關資料可能被濫用的情況保持警覺。衞生署於2008年4月25日舉行記者招待會，就事故向公眾致歉及公布各項跟進行動。該署並設立電話熱線，處理這方面的公眾查詢；

(b) 該署已更新有關使用電腦及資訊科技系統可抽離資料儲存裝置的常務通告，提醒員工除非情況特殊，並已獲得服務單位主管批准，否則不得把可識別身份的個人資料儲存於這類裝置內。儲存於這類裝置的個人資料和數據必須加密，並應盡量把所儲存的相關資料減至最少，能應付運作需要便可。使用完畢後，應立即刪除資料；及

(c) 該署為部門首長、行政人員及資訊科技保安人員舉辦有關資料保護和辦公室保安的研討會，藉以加強員工的認知。

警務處

7. 警務處監管處處長表示，關於載有敏感的行動資料及19名人士個人資料的文件透過Foxy軟件(即點對點檔案共享應用軟件)在網上洩露的事故，警方會以非常嚴肅的態度對待。他就資料外洩致歉，並向委員簡述以下事項：

(a) 調查發現，由於個別警務人員未有遵從《警察通例》下有關資訊保安和保護個人資料的規定，導致資料在網上洩露。目前並無證據顯示警方的資訊科技系統遭到破壞；

(b) 除傳閱相關指引外，該處亦舉行訓示會，提醒員工有關資訊保安的重要性及使用檔案共享應用軟件的潛在風險。根據2008年5月27日發出的指示，所有員工應於2008年6月初之前，從他們的個人電腦移除警方的資料。該處亦會提醒員工有關使用Foxy檔案共享應用軟件的危險；及

(c) 警務處副處長(行動)轄下已成立工作小組，全面檢討資訊科技保安，並研究辦公室的電腦是否足夠，以及在家裏使用個人電腦工作的事宜。

公務員事務局

8. 公務員事務局副秘書長3向委員簡報有關紀律研訊個案的資料外洩事故，以及當局採取的補救行動，內容綜述如下：

(a) 2008年4月23日，該局發現遺失一枚便攜式電子儲存裝置，內有兩宗紀律研訊個案的資料，當中涉及25名在職公務員的姓名和職銜。該局已向警方報案及向私隱專員報告，並向有關的25名公務員致歉；

(b) 該局進行調查後，已向遺失上述資料的人員作出警告；

(c) 該局已檢討及加強對使用和存放載有個人或受限制資料的便攜式電子儲存裝置的保安措施，而且透過訓示和通告，提醒員工時刻遵守有關的指引和規例；及

(d) 該局提醒員工不可使用便攜式電子儲存裝置下載、儲存或傳送受限制資料。該局亦指示員工，在任何情況下均不得把受限制資料帶回家。如確有需要，員工應事先取得批准及只可使用由該局提供和備有適當防護功能的裝置。如有需要，該局可提供保密網絡，備有加密及認證功能的虛擬專用網絡筆記簿型電腦，供員工使用。

個人資料私隱專員公署

9. 私隱專員表示，公署負責監察《個人資料(私隱)條例》(第486章)(下稱《私隱條例》)的施行，該條例同時涵蓋私營及公營機構，包括公共機構。每名市民和資料使用者(包括公務員)有責任遵守《私隱條例》。就此，他指出政府當局的文件(立法會CB(1)1679/07-08(01)號文件)顯示，直至發生資料外洩事故之前，政府資訊科技總監辦公室並無採取積極步驟，提醒政府所有員工有責任遵守《私隱條例》的規定。政府當局於2008年5月8日發出的通告內，才首次宣布有關匯報資料外洩的安排。故此，私隱專員質疑政府當局在推廣遵守《私隱條例》方面的決心和承擔。

討論

通知受資料外洩事故影響的資料當事人

10. 劉慧卿議員對近期多個政府政策局和部門及滙豐銀行的資料外洩事故感到失望，這些事故令社會深感不安。她又深切關注到，互聯網上洩露了警方的敏感行動資料，對資料當事人可能造成的嚴重後果。她詢問，所有受資料外洩事故影響的人士是否已獲得通知，有關的政策局和部門及公共機構又會否一如滙豐銀行，承諾對受事故影響的資料當事人蒙受的任何損失負責。

11. 醫管局財務總監、衞生署助理署長(特別衞生事務)及公務員事務局副秘書長3回應時表示，所有受近期事故牽連的資料當事人已獲告知其資料外洩，並獲提醒對其資料可能被濫用保持警覺。就入境處的個案而言，入境處助理處長(資訊系統)表示有14人受影響，當中11名為外來訪客，3名為本地居民，其聯絡資料不詳，未能作出跟進。受資料外洩影響的人士如認為有需要，可向入境處提出書面申索。警務處監管處處長表示，警方已按照警務處處長指示，採取行動通知受資料外洩影響的人士。該4份在互聯網上曝光的文件共涉及19名資料當事人。由於文件沒有載列足夠的詳細資料，故此需要一些時間，以確定有關人士。

12. 劉江華議員察悉，過去3年發生了30宗資料外洩事故，涉及約44 000名資料當事人，但只有7個政府部門和公營機構曾通知受影響的市民。他關注政策局和部門選擇性地通知受影響的市民，又欠缺劃一的做法，用以警惕受資料外洩影響的資料當事人。

13. 政府資訊科技總監答稱，個別政策局和部門會按個別情況，決定應否通知資料當事人。在即將進行的檢討中，將會研究應否強制規定須通知受資料外洩影響的資料當事人，以及例外情況可否獲得特別考慮。

14. 關於向受資料外洩影響的人士作出賠償，私隱專員表示，資料當事人的個人資料被洩露，可循民事法律程序尋求損害賠償。他表示，目前並無法例條文或資源讓私穩專員公署協助資料當事人申索賠償。

對造成資料外洩的人員採取紀律處分

15. 對於若干政策局局長不出席是次會議，就其職權範圍下的部門／公共機構發生資料外洩，回應公眾和委員提出的關注，王國興議員感到失望。他要求政府當局和醫管局交代如何處理個人資料被濫用的個案，以及有否對沒有遵守部門指引的人員採取紀律處分。他亦詢問有何措施保障私隱和保護個人資料。

16. 劉慧卿議員贊同王議員的看法，並要求當局對資料外洩事故進行獨立調查，冀能建議全面的改善措施，防止事故重演。

17. 公務員事務局副秘書長3回應時表示，政府當局極之關注個人資料外洩。牽涉資料外洩的部門／機構已經完成或正在徹底調查該等事故。她向委員保證，在進行調查後，將會按照公務員既定的紀律機制，處理任何違反和不遵從規例的人員。醫管局財務總監確認正在調查資料外洩事故，並會按照當前的人力資源政策，對違反既定的保安指引和人事政策的人員採取適當行動。

18. 警務處監管處處長告知委員，所述個案已轉交商業罪案調查科的科技罪案組進行全面調查。對於不涉及刑事成分的個案，將會視乎適當情況展開紀律程序。任何人員如被發現違反警方內部指引，將會受到按既定程序採取的紀律處分。這些罰則可以是勸喻甚或解顧，視乎違規的性質和嚴重程度而定。

監察檔案共享應用軟件

19. 因應涂謹申議員詢問如何監察檔案共享應用軟件，入境處助理處長(資訊系統)答稱，部門的資訊科技系統定期接受風險評估及內部保安審計。入境處一直密切監察情況，以確定在互聯網能否透過檔案共享應用軟件的搜尋器，找到部門的任何受限制資料。

20. 警務處監管處處長表示，警方進行網上巡查，監察Foxy及其他點對點檔案共享應用軟件，以找出在互聯網流傳的任何受限制資料，並會即時採取行動，移除該等文件。但他指出，這些文件一旦傳送至其他各方，則難以徹底刪除。

21. 政府資訊科技總監補充，一隊保安小組會每天監察互聯網，搜尋在互聯網可能透過軟件通用形式流傳的政府文件。

採用先進的保護資料科技

22. 楊孝華議員認為，鑒於互聯網和便攜式電子儲存裝置的使用既方便又普遍，與其禁止使用這類裝置和不准把工作帶回家，倒不如加強教育工作，加深員工對資訊保安的認知及其對安全使用這類裝置的知識。他以網上銀行的自動切斷連線為例，建議採用最新的保護資料科技，利便員工在安全的電腦使用環境下工作。

23. 劉江華議員要求當局提供資料，說明將會採取的具體措施防止進一步洩露資料，以恢復公眾對政府處理個人資料的信心。

24. 政府資訊科技總監回應時表示，從最近的事件中，在家裏工作是一個明顯的風險來源。為使經授權的政府人員基於運作需要可在辦公室以外的地方工作，當局採取了各種科技方案。這些方案包括使用備有加密和密碼鎖定功能的加強版USB閃存盤(在醫管局使用)；提供保密網絡，備有加密及認證功能的虛擬專用網絡筆記簿型電腦(在公務員事務局使用)；以及有保安及防止擅用功能的應用軟件。至於Foxy點對點檔案共享應用軟件，政府資訊科技總監表示，雖然資訊科技資產管理科技有助確保未經授權的應用軟件不會被上載到政府資訊系統，或防止任何未經授權的資訊系統設備被接駁到政府資訊系統，卻難以阻止有關員工在家庭電腦安裝這類軟件。因此一般的規條是，建議員工不要複製或把載有受限制及個人資料的官方檔案帶回家。鑒於近期大部分事故的起因是這類在家裏未經授權的作為，當局建議所有政策局和部門研究這類作為的風險和影響，並建議政策局和部門採取適當措施減低風險，以及確保經授權的員工獲提供安全的電腦使用環境，可在家裏工作。

25. 然而，政府資訊科技總監強調，科技和程序可以做的總有極限，沒有一種技術方案可保證提供100%的資料保護。由於在電腦使用環境下受到的很多保安威脅都是人為因素造成，當局會加強培訓和教育項目，以營

造保護資料的文化和承擔，並加深員工對保安問題的認知，使他們知道如何遵守相關的資訊保安規定。政府資訊科技總監辦公室和保安局在公務員事務局的支援下，將會與部門資訊科技保安主任緊密合作，設計一套員工溝通項目，旨在使所有在辦公室以外的地方及／或家裏工作的員工，建立和維繫對處理官方文件的高度認知、警覺性和承擔。

26. 醫管局醫療信息總監表示，鑒於近期發生遺失便攜式電子儲存裝置個案，醫管局已提升病人資訊系統，令下載的可識別病人身份及個人資料的病人資料須以加密程序保護。此外，強制員工使用備有加密和密碼"鎖定"功能的加強版USB閃存盤，以保護病人資料。

檢討資訊保安政策及規例

27. 政府資訊科技總監表示，政府當局會因應對事故的調查結果，在未來3至4個月，檢討資訊保安政策和規例、保安審計的內容、角色和責任，確保整個公營機構界別的資訊保安。政府當局亦會向政策局和部門及公共機構提供指引，要求它們因應本身的特定運作需要，按照指引和《私隱條例》的條文訂立各自的保護資料措施。

28. 主席詢問有何保安指引和措施，防止將會離職的人員儲存個人資料作私人用途。政府資訊科技總監答稱，此舉屬濫用個人資料，違反《私隱條例》及公務員／公共機構的保安指引，當局會對這些個案實施執法和紀律處分。助理政府資訊科技總監(基礎設施及資訊保安)表示，當局規定全體公務員在使用該等資料後，須即時從他們的個人電腦刪除上述資料，而政策局和部門須負責監察員工的遵守情況。醫管局財務總監表示，業已制訂有關儲存媒體的保安和棄置、人事程序的既定指引，規定即將離任的員工交還辦公室資產，包括他們所管有的資料。公務員事務局副秘書長3表示，根據保護資料原則之下的規定，業已就保留與員工招聘及委任有關的個人資料設定時限。私隱專員指出，違反《私隱條例》的保護資料原則及為個人得益而不正確使用資料，不屬刑事罪行。公署已向政府當局建議，對《私隱條例》引入修訂進行公眾諮詢，這些修訂包括把任何人未經資料使用者同意而取得、披露或售賣資料使用者所持有的個人資料，訂為刑事罪行。

個人資料私隱專員的權力及職能

29. 因應私隱專員質疑政府當局對推廣遵守《私隱條例》的承擔，政府資訊科技總監答稱，每名資料使用者(包括政府及非政府機構)有責任遵守《私隱條例》的法例規定。他強調，政府極之重視保安規定和《私隱條例》的保護資料原則。為此，當局於2008年5月8日向全體公務員發出通告，提醒他們有責任遵守《私隱條例》的規定。政府資訊科技總監辦公室發出的基準資訊科技保安政策亦參考了《私隱條例》。公務員事務局副秘書長3補充，公務員事務局於2002年8月發出詳細指引，述明在與僱傭事宜有關的個人資料方面如何遵守《私隱條例》。事實上，政府已向所有政策局和部門發出多份通告，闡釋《私隱條例》的條文，確保它們遵守這項法例。

30. 王國興議員對私隱專員公署沒有權力，似乎是一隻"無牙老虎"感到失望。郭家麒議員認同王議員的看法，並關注私隱專員公署作為政府資助法定機構，負責保障個人資料的安全和保護，卻須依賴傳媒報道以獲得資料外洩事故的資訊。劉江華議員表示，私隱專員公署除了在接到投訴後採取行動，亦獲《私隱條例》賦權主動調查任何涉嫌資料外洩事故。就此，王國興議員、郭家麒議員及劉江華議員要求當局提供資料，說明私隱專員已經／將會採取的措施和行動，以保護私隱和資料安全。

31. 私隱專員回應時表示，公署只有39名員工，沒有足夠資源監察所有機構，預先防範可能發生的資料外洩事故。私隱專員公署迄今只接到一宗投訴，涉及基督教聯合醫院(下稱"聯合醫院")一名僱員遺失載有26名病人資料的USB閃存盤。公署未有接獲對其他醫院、公共機構、政策局和部門遺失資料的投訴。他強調，資料外洩事故經傳媒曝光後，公署已在其能力範圍內即時採取行動。除了聯合醫院的事故正在調查中，他已決定採取前所未有的步驟，行使《私隱條例》賦予的視察權力，視察公營醫院的個人資料系統。私隱專員公署亦已展開循規查察行動，包括調查近期多家公營醫院和診所、衞生署、入境處、公務員事務局和警務處的資料外洩事故，以及滙豐銀行某分行在進行翻新工程期間，遺失載有客戶資料的伺服器的個案。完成調查後，便會發表報告和提出建議。

32. 在教育和培訓方面，私隱專員特別指出，公署已充分利用這筆用作推廣和教育的64萬元有限撥款。從2007年到現在，為公眾舉行了共17次研討會、為機構(包括醫管局)籌辦了93次講座，全部大受歡迎，有超過10 000

人出席。然而，儘管2008-2009年度增加撥款100萬元，但這筆撥款僅足夠製作一齣政府宣傳短片／聲帶。若獲得更多資源，公署將可就資料保護及保安展開更多預防性的教育和培訓項目。

33. 私隱專員又指出，12年前制定《私隱條例》時，立法者決定由《私隱條例》訂明私隱專員的權力範圍。現時並無法例條文規定資料使用者向公署報告個人資料外洩事故，而公署亦只能夠在傳媒查詢和報道時，才得悉這些事故。他促請政府當局認真考慮作出良好的處事方式，要求政府部門向公署報告這些事故，以便及時跟進。由於公署早前曾向政制及內地事務局建議修訂《私隱條例》，他促請立法會議員在即將進行的《私隱條例》檢討中，支持擴大私隱專員的權力。就此，政府資訊科技總監表示，政府當局會考慮應否強制規定向私隱專員報告資料外洩事故。

員工把工作帶回家

34. 涂謹申議員詢問，入境處和警方有否評估員工在放工後，把機密／受限制文件帶回家裏工作的普遍程度。他要求當局澄清，入境處員工能否從部門的資訊科技系統下載這類文件。

35. 入境處助理處長(資訊系統)回應時表示，入境處的入境／出境紀錄及個人資料的資訊科技系統沒有與外界連線，因此不能把檔案／文件下載或上載到互聯網。她強調，部門的既定政策是，除非情況特殊及事先取得批准，否則不得把機密文件及檔案帶離辦公室。員工一般寧願在辦公室超時工作，亦沒有員工要求把載有個人資料的文件帶回家裏工作，因為他們須參考的文件實在太多。該處定期傳閱有關資訊保安及保護個人資料的指引、規例和指示，以加深員工的認知。為確保有安全的電腦使用環境，經授權的員工獲提供備有加密及認證功能的筆記簿型電腦，讓他們基於運作需要而在家裏工作。

36. 涂謹申議員提到各種加強版的保安裝置，例如醫管局使用備有加密和密碼"鎖定"功能的加強版USB閃存盤，以及公務員事務局使用虛擬專用網絡筆記簿型電腦。他詢問，在等待工作小組進行檢討期間，警方會否為員工作出類似安排。

37. 警務處監管處處長回應時表示，在等待資訊科技保安的全面檢討結果期間已引入多項臨時措施。這些措施包括一項大型行動，確保親自訓示每名員工從他們的個人電腦移除警方資訊，以及提醒有關點對點檔案共

享應用軟件的危險。在提供電腦設施方面，警務處監管處處長表示，警方現時有超過13 300台電腦，當中9 736台電腦已接駁網絡。督察級和以上職級的人員乃至有運作需要的初級人員均獲編配電腦。另外設有終端機，方便共用。他特別指出，過去兩年，電腦的數量已由7 000台增加至超過9 000台。管理層會檢討有否足夠電腦供員工使用，如資源許可及有充分的需要，將繼續把電腦升級和增加供應。警方亦會評估員工把工作帶回家的普遍性，並研究箇中原因。

38. 劉江華議員認為，把洩露資料的全部責任歸咎前線人員，殊不公允，亦不負責任。他提到警方的情況時指出，200名前線警務人員要共用警署內的4台電腦，由於工作繁重和資源不足，警務人員有實際需要把工作帶回家。他認為資料外洩事故是警方失職。管理層應檢查和監察如何使用受限制文件，並警惕員工有關點對點檔案共享應用軟件的潛在危險。劉議員詢問當局會實施甚麼即時改善措施，減低進一步洩露資料的風險。他又促請當局全面檢討在家裏使用個人電腦處理公務事宜。

39. 警務處監管處處長表示，不同種類的警務工作對電腦的需求亦有所分別。由於大部分人員是執行前線及非伏案的職務，故此某些人員會獲得優先使用電腦。督察級和以上職級的人員乃至有運作需要的初級人員均有指定的電腦終端機，其他人員則使用公共終端機。此外，現時並無規定須使用文字處理的軟件擬備報告／供詞，手寫的報告／供詞已經足夠。他強調，在即將進行的檢討中，管理層會研究把工作帶回家的原因，評估有否真正需要這樣做，以及檢討把工作帶回家是否因辦公室電腦數量不足或因個別人員的工作習慣所致。他特別指出，管理層察悉員工對電腦的需求。事實上，電腦的數量在近年已穩步上升。如資源許可及有充分的需要，警方會繼續盡力提供足夠的電腦數量，供員工使用。應委員要求，警務處監管處處長答允在適當時間向事務委員會匯報已實施的改善措施。

40. 政府資訊科技總監同意，管理局在某程度上亦須承擔洩露資料的責任。鑒於近期大部分事故的起因是員工未經授權而在家裏工作，當局會致力處理導致資料外洩的人力和管理問題，並加強執行措施及強化內部管理，確保員工遵守相關保安規例和指引。就此，當局已要求所有政策局和部門瞭解事件，並建議員工不要把受限制資料帶回家。各政策局和部門亦應確保獲授權在家裏工作的人員獲提供安全的電腦使用環境。

經辦人／部門

41. 郭家麒議員察悉，除了在醫院長時間照顧病人的服務外，有關研究和資料整理的額外工作量亦令許多醫院員工須把工作帶回家。他詢問醫管局每年的資訊科技保安預算，並要求提供詳細資料，說明為醫院員工提供資訊科技支援、資料保護及資訊科技保安的培訓。

42. 醫管局財務總監回應時表示，資訊科技保安是醫管局資訊科技／資訊服務基礎設施的重要部分，以支援臨床管理運作系統。要劃清資訊科技保安的預算，實在有困難。然而，資訊科技預算包括了資訊科技服務撥款的經常及發展開支，撥款約佔醫管局總預算的1.6%至1.7%。她特別提到，醫管局向來設有一個包括防火牆、防止入侵保護及劃一資源位址過濾系統的安全網絡基礎設施，以免個人資料遭受他人在未獲授權情況下查閱及惡意入侵。發生資料外洩事故後，醫管局已提升病人資訊系統，令下載的病人資料自動得到加密程序保護；並且推行使用備有加密和密碼"鎖定"功能的加強版USB閃存盤。在提供資訊科技設施方面，她表示，醫管局約有2萬台電腦，足夠員工使用。醫管局獲悉事故之前，已透過通告、通訊、小冊子、醫管局內聯網，向前線員工公布資訊保安政策指引，以及為醫院員工舉辦資訊科技研討會和簡報會。對於新入職員工，特別是醫院員工，醫管局在入職簡介中向他們介紹對病人資料保密的責任及資訊科技的保安事宜。醫管局為實習醫生提供有關使用臨牀管理系統的培訓中，亦包括對病人資料保密的責任和資料查閱管制的課題。在發生該等事故後，醫管局發出"有關加強執行個人資料保安措施"及"有關處理遺失載有可識別病人身份的個人資料的電子器材事件的政策"的工作通告，提醒員工保障個人資料的重要性；並推出保護病人資料的宣傳片及複修課程，以教育醫管局員工有關這方面的知識。每個醫院聯網設有資訊科技委員會，負責資訊科技事宜，並會向員工提供支援。醫管局財務總監強調，管理層會致力向員工提供所需的資訊科技支援。

43. 郭家麒議員表示，資訊科技委員會主要由義工組成，沒有任何經費。他認為，管理層應為員工提供培訓課程及面對面的支援和建議。

政府當局

44. 郭家麒議員及劉慧卿議員要求政府資訊科技總監辦公室負責統籌，要求各政策局和部門及在它們職權範圍內的公共機構／大專院校作出回覆，以列表方式摘要述明過去3年的資料外洩事故。政府資訊科技總監辦公室亦應告知事務委員會受影響資料當事人的數目，有否知會受影響市民／私隱專員／警方，以及沒有通知有關方面的原因。

(*會後補註*：政府當局提供的過去3年個人資料外洩事故摘要，已於2008年6月13日隨立法會CB(1)1875/07-08號文件送交委員。摘要載列了30宗事故，在24宗事故中，有關政府部門和公營機構有知會受影響市民。有關沒有知會市民的個案，主要原因是聯絡資料不詳。)

45. 劉慧卿議員詢問，政府當局有否制訂關於員工把工作帶回家的政策。她表示她個人反對這做法，但若基於運作需要，必須把工作帶回家，則政府當局／管理層應訂明清晰指引，制訂措施為員工提供安全的電腦使用環境，確保在家裏和辦公室之間安全傳送資料。

46. 政府資訊科技總監表示，每個政策局和部門將須按照本身的運作要求，自行決定有關在家裏工作的政策和安排。但他指出，在家裏使用個人電腦處理公務，並以可抽離儲存裝置在辦公室和家裏之間轉移資料，顯然構成外洩資料的風險。若允許在家裏工作，管理保安風險的較佳方法，是在虛擬專用網絡平台提供保密網絡連線，此舉類似入境處和政府資訊科技總監辦公室作出的安排，從而無需在可抽離儲存裝置下載資料。政府資訊科技總監補充，若把個人及敏感資料存儲於可抽離USB閃存盤，則必須加密。當局會安排會議，向部門主管作簡介，並要求他們檢討在家裏工作的安排，以盡量減低資料外洩的風險。

47. 警務處監管處處長表示，一般的規條是不鼓勵在家裏工作。警司和以上職級的人員，乃至證明有需要及基於運作理由獲授權在家裏工作的總督察，均獲提供安全的電腦使用環境，在虛擬專用網絡平台把辦公室和家裏連線。警方會檢討這項政策，以確定有否需要把督察職級也包括在內。

48. 公務員事務局副秘書長3表示，政府當局沒有制訂在家裏工作的政策，這主要是個別人員的做法。該局建議員工，在任何情況下均不得把受限制資料帶回家。如確有需要，員工應事先取得批准及只可使用由所屬政策局和部門提供的備有適當防護功能的裝置。如有需要，有關政策局／部門可提供保密網絡，備有加密及認證功能的虛擬專用網絡筆記簿型電腦，以供使用。

49. 醫管局醫療信息總監表示，根據醫管局的指引，員工不得把可識別個人資料儲存於家庭電腦。經授權在家裏工作的員工獲提供虛擬專用網絡設施。

50. 衞生署助理署長(特別衞生事務)表示，該署原則上不鼓勵員工把受限制資料和敏感資料帶回家裏處理。他表示，該署在診所和中心設有足夠的電腦，供員工使用。如有需要，會為出勤到辦公室以外的地方工作的員工提供備有保安措施的筆記簿型電腦。

51. 涂謹申議員提到政府當局表示不鼓勵員工在家裏工作。他認為這些言論帶有侮辱性和打擊士氣，會造成前線人員與管理層之間的衝突。他認為，資料外洩事故的部分成因是欠缺資源和工作繁重。以警方為例，他表示初級人員由於辦公室沒有足夠電腦可供使用，故此被迫把工作帶回家，以完成文書工作。有鑒於此，有關人員不應獨力承擔責任，反而應獲提供技術協助，在安全的電腦使用環境下在家裏工作。他表示，即使發出額外指引，也不能解決問題。他促請警方購置更多配備文字處理功能的電腦，以供輸入受限制資料，並為員工提供具體的技術支援。警務處監管處處長察悉涂議員的建議。

52. 主席作出總結，要求政府各代表向局長轉達委員對他們不出席這次會議感到失望。劉議員建議在7月初本立法會會期結束前舉行事務委員會會議，並邀請發生資料外洩的政策局的局長匯報採取跟進行動及推行補救措施的進度。議員表示同意。

(*會後補註*：由於商務及經濟發展局局長未能出席2008年7月8日舉行的特別會議，政府當局亦表示，近期發生的個人資料／受限制文件外洩事故沒有進一步的最新發展。經諮詢部分事務委員會委員後，主席指示，2008年7月8日的特別會議將不會舉行。)

II. 其他事項

53. 議事完畢，會議於上午11時05分結束。

立法會秘書處
議會事務部1
2008年9月24日