二零一零年七月十二日

參考文件

立法會資訊科技及廣播事務委員會

資訊保安

目的

本文件告知委員自上次二零零九年七月十三日匯報至今，政府在資訊保安改善計劃方面的進展。

背景

2. 政府繼續致力改善各決策局／部門(局／部門)的保安措施，並支持社會各界改善其資訊保安狀況。各項保安措施及最新狀況，分別按下列三個主要範疇匯報 -

(a) 政府的資訊保安改善計劃；

(b) 政府的資訊保安狀況；以及

(c) 公眾的資訊保安。

政府的資訊保安改善計劃

3. 要管理資訊保安，防預工作是成功的一大要素。資訊保安改善計劃的目的是要增強員工的資訊保安認知和教育；豐富技術和程序措施；規範保安風險評估和監察；以及檢討保安規例、政策和指引。

(i) 員工的資訊保安認知和教育

4. 政府資訊科技總監辦公室在二零零九年四月起，透過多種溝通方法和渠道[1]，推行了爲期一年有關資訊保安的員工溝通計劃，並得到員工良好的反應。其中一項活動是在各政府辦公大樓舉行的連串巡迴展覽，獲得超過 12 000 名員工參與。我們還定期舉辦由政府資訊科技總監辦公室統籌的培訓課程，也協助各局／部門設計自用的培訓項目，以應付他們不同的需要，例如爲新入職的行政主任舉辦資訊保安簡報會，作爲其入職課程的常設項目。

5. 爲了評估計劃的成效，我們在計劃前和計劃後均進行了統計調查。結果顯示，員工在資訊保安知識和態度上都有明顯改善。例如，在計劃推行後，受訪者中有閱讀過資訊科

[1] 包括製備和分發單張、海報和醒目提示；舉辦研討會和網上培訓課程；製作錄像培訓教材和動畫；在員工通訊刊載文章；以及舉辦巡迴展覽，讓政府各級員工參與。

技保安政策文件至少一次者的比率，多了接近一倍。同時，對各種嶄新的資訊保安威脅有更深入理解者的比率，也增加了超過一倍。

6. 鑑於社會各界更廣泛使用社交網絡，而政府在一些公務上使用社交網絡的情況也日漸增多，我們已就資訊保安威脅和防護措施發出具體指引。我們也提醒員工須審慎處理和棄置可能在使用時儲存敏感資料的內置電子設備，包括新一代辦公室儀器如複印機、傳真機和打印機等。

(ii) 技術和程序措施

7. 政府資訊科技總監辦公室繼續密切留意與資訊科技發展趨勢相關的風險和市場推出的技術解決方案，以協助各局／部門採取適當的措施來保護他們的資訊系統和資料。政府資訊保安事故應變辦事處的常設辦公室亦定期發出保安和病毒警報，提醒各局／部門在管理和營運其資訊系統和資料庫時，必須及時進行軟件修補，以堵塞保安漏洞，以及遵行良好的資訊保安作業模式。

8. 在政府資訊科技總監辦公室的協助下，一些局／部門已因應其不同的保安需要，成功開發和推行其資訊系統保安

方案，以進一步加强遠端存取和終端用戶的設備及連接[2]。例如，香港警務處 (下稱"警務處") 已採取多管齊下的措施，包括加強端點保安監控，提供加密的便攜式儲存裝置及有嚴格保安規限的筆記簿型電腦作公事用途，並推行虛擬工作站計劃，以支援警務人員使用流動電腦設施的工作需要。警務處向員工提供培訓和定期傳達訊息，以便向他們灌輸有關資訊保安的知識，並使他們明白資料外泄所涉及的風險。警務處亦增加對各種資訊系統、用戶循規情況和共用電腦設備進行保安審計的次數。

(iii) 加強管理以確保各方遵行資訊保安規定，並向各局／部門和公共機構提供意見及支援

保安風險評估和監察

9. 根據現行的資訊科技保安政策，各局／部門須定期進行保安風險評估和審計。政府資訊科技總監辦公室已對部門保安風險評估的程序作出檢討和修訂，並向各局／部門公布最新指引。

10. 爲優化由政府資訊科技總監辦公室統籌進行的循規

[2] 包括使用各種技術措施，例如虛擬私有網絡解決方案可提供安全的遠端存取，端點保護解決方案可助建立存取監控政策，以及虛擬化技術有助建立一個安全的電腦運作環境。

監察及審核程序，我們在二零零九年年底，修訂了監察機制，包括提高關注特定或重要範疇、透過調查收集資料、進行抽樣審查和整合各局／部門的保安風險評估結果。通過這些安排，我們可加深了解和更密切地監察各局／部門的保安狀況和循規情況，以及使各局／部門能更積極主動偵測和解決保安問題。這項新機制會在二零一零年第四季開始運作。

公共機構

11. 各局／部門及其轄下的公共機構繼續就資訊保安事宜交流有關資訊，並統籌推行適當的保安措施，以應付資訊保安風險。在二零一零年五月，政府資訊科技總監辦公室向各局／部門發出催辦便箋，要求他們提醒其轄下的公共機構關注常見和當前的保安威脅，其中包括仿冒詐騙、惡意程式碼攻擊和遺失便攜式存儲裝置。我們已在催辦便箋內提供有關保護資訊系統免受這些威脅的實用提示和技巧。

12. 醫院管理局繼續採取必要的措施，以加強資訊保安和緩解資料泄漏風險。有關工作進展的摘要請參閱**附件 1**。

(iv) 檢討資訊保安規例、政策和指引

13. 政府資訊科技總監辦公室於去年檢討了政府保安規

例的資訊科技範疇，並公布更新的規定給各局／部門遵行。其中一項改變是強制通知規定。自二零零八年年底，如有保安事故涉及個人資料，有關的局／部門必須盡快向個人資料私隱專員公署報告，並在切實可行範圍內盡量通知受影響人士。爲確保有關規例、政策和指引能與時並進，爲配合科技的進步、國際的發展和業界的良好作業模式，並能協助應付嶄新出現的保安威脅，我們還納入了新興的保安課題，包括端點存取監控，並更新了良好作業模式，例如使用最新的加密標準將 Wi-Fi 訊息加密。

政府的資訊保安狀況

14. 雖然我們無法完全阻止保安事故發生，但這些事故出現的次數已有減少的迹象。在二零一零年首兩季，政府資訊保安事故應變辦事處接獲了四宗資料泄漏保安事故報告[3]。

15. 自上次本委員會會議於二零零九年七月舉行後的 12 個月內，政府資訊保安事故應變辦事處共接獲八宗資料泄漏事故報告。這些事故的摘要載於**附件 2**。在這些事故之中，一宗不涉及敏感資料。就其他兩宗涉及遺失儲存媒體的事故而言，有關遺失媒體內的資料已經過加密處理或受到存取控

[3] 在二零零九年，當局全年接獲 14 宗保安事故報告，其中十宗屬資料泄漏事故。

制機制保護。而所有涉及個人資料的事故，有關的局／部門已向個人資料私隱專員報告，並適當地通知受影響人士。

公眾的資訊保安

社會各界活動

16. 爲了推動互聯網服務供應商對網絡保安工作的支持，政府資訊科技總監辦公室定期聯同警務處和香港電腦保安事故協調中心(下稱“協調中心”)，就時下各種課題舉辦互聯網服務供應商研討會，目的是要讓互聯網服務供應商知悉那些可能會影響其運作的嶄新網絡保安威脅，以及讓互聯網服務供應商、協調中心和執法機關分享心得，並討論如何合力應付該等攻擊，爲社會帶來裨益。爲了測試本港主要的互聯網基建持分者在重大事故發生期間的協調情況，協調中心和有關方面計劃在二零一零年十月進行一項資訊保安事故應變演習。

17. 二零零九年“全城電腦清潔日”活動已順利舉行。該活動以主題爲“網上交易安全”的公眾會議作爲終結。會後調查顯示，超過 90%受訪者給予很高評價。我們已開展二零一零年“全城電腦清潔日” 活動，於三月和五月舉辦了兩場免

費的公眾研討會，並將於十一月再舉辦，主題暫定爲"安全網上社交網絡活動"。

18. 我們已製作供電台播放的宣傳聲帶，提供有關資訊保安的實用小提示和良好作業模式。在最近數月，我們製作了以社交網絡安全爲主題的宣傳聲帶。我們亦已在一站式資訊保安網站(www.infosec.gov.hk) 刊載文章，以協助電腦用戶了解使用網上社交網絡服務的保安問題，並提醒青少年小心網絡保安威脅，例如網上誘拐和網上欺凌。政府亦於二零零九年九月，推出了爲期一年的互聯網教育活動，向學生、家長和老師推廣安全及正確使用互聯網的訊息。

嶄新的網絡保安威脅

19. 世界各地正面對惡意程式碼、蠕蟲和殭屍網絡[4]等網絡保安威脅。政府與有關各方繼續攜手合作，協力提高社會各界的資訊保安認知，使商界和市民明白保護其電腦資產的重要性。自二零零八年年底起，一種惡名昭彰的電腦蠕蟲[5]令很多地方的電腦廣泛受到感染。政府資訊科技總監辦公室一直與香港互聯網註冊管理有限公司、協調中心和警務處合作，密切留意有關的事態發展，並偵測任何可影響本港的活

[4] 殭屍網絡是指被操控的電腦所組成的網絡。這些電腦均在擁有者不知情的情況下被遠程操控，在網上進行惡意活動。

[5] 電腦蠕蟲名爲「飛客」。

動迹象。透過上述合作，我們會在有需要時向可能受影響的用戶提供建議。

20. 我們察悉惡意程式碼不斷在多人使用的流動平台上出現。隨着市民廣泛使用流動通訊設備，惡意程式碼感染所造成的影響越趨顯著並產生連鎖反應。我們正密切留意國際和本地組織所提供的電腦保安資訊，以便掌握有關電腦保安攻擊和防禦方案的最新趨勢。我們會透過一站式資訊保安網站與市民分享有關資訊。

總結和未來路向

21. 政府去年繼續推行各項改善計劃和活動，以維護我們的資訊保安狀況。嶄新出現的保安威脅、新的業務計劃、先進科技的採用，以及互聯網上不斷改變的服務模式，都帶來不斷演變和新的資訊保安風險。維持高水平的資訊保安狀況，會是一項具挑戰性的工作。我們定當時刻保持警惕，竭力保護政府的資料資產。

22. 我們注意到員工對資訊保安基本訓練課程的需求甚殷，因此會在來年舉辦更多同類課程。我們會採用新的機制，以加強對各局／部門的保安監管。透過舉辦公眾認知和

教育活動，我們繼續協助市民提升防禦網絡保安威脅的能力。資訊保安不是一次過便能完成的項目，而是一個需要反覆進行的過程，在人事、程序和技術方面均須互相配合。我們會按年向委員匯報各項保安措施的進展。

徵詢意見

23. 請委員察悉本文件的內容。

商務及經濟發展局

政府資訊科技總監辦公室

二零一零年七月

附件 **1**

資訊科技及廣播事務委員會
二零一零年七月十二日會議

有關醫院管理局所採取行動的進展

目的

本文件向委員簡報自二零零八年遺失病人資料事件發生後，醫院管理局(下稱“醫管局”)在加強保障病人資料安全及私隱方面所採取行動的進展。

背景

2. 醫管局專責小組(下稱“專責小組”)及個人資料私隱專員(下稱“私隱專員”)分別就八個範疇提出了 26 及 37 項建議，以進一步加強保障病人資料安全。有關範疇包括醫管局的政策、架構及人事、員工在私隱保安意識方面的培訓、程序及指引、私隱影響評估、監察及審計、合約、以及科技。醫管局已就有關建議制訂和實施行動計劃，以處理有關問題。

行動計劃及進展

3. 醫管局大會於二零零八年九月批准醫管局就專責小組和私隱專員的建議，採取涉及 19 個綜合目標的行動計劃，以加強保障病人資料安全及私隱。

4. 以下是已採取的行動撮要：

(a) 爲有效監督資訊保安及私隱改善計劃在醫管局總辦事處及聯網的推行情況，醫管局成立了監管架構，即醫管局資訊保安及私隱委員會和聯網資訊保安及私隱委員會，以監督有關工作目標在整個醫管局的落實情況，務求加強該局的資訊保安及私隱。

(b) 除了加強監管資訊保安及私隱外，醫管局和私隱專員還合作在各間醫院推行加強私隱意識運動，以提高醫管局員工的私隱意識，從而加強保護病人的資料私隱。在二零零九年五月至二零一零年三月期間，醫管局和私隱專員舉辦了一些有關的研討會。

(c) 醫管局已在二零零九年爲轄下所有員工製作網上學習課程，作爲標準教育單元，以提供《個人資料(私隱)條例》所訂有關保護個人資料，以及醫管局資訊保安及私隱政策的基本知識。醫管局要求員工須在二零一

零年年底完成該課程。

(d) 爲協助員工在工作間保護病人資料私隱，醫管局已檢討及更新有關資訊保安及私隱的程序及指引。該局會持續並有計劃地，以有效的方式公布該些程序及指引。

(e) 在存取審計系統推行後，醫管局已於二零一零年第一季對病人資料的存取進行審計。該局日後將定期進行審計，以偵測可能違規的資料的存取情況。

(f) 醫管局已實施科技改善措施，保護下載中的資料和在高風險工作站中的資料，以防止資料外泄。並計劃進一步加強工作站的保護措施。

5. 一些行動計劃目標已逐步落實，但由於落實過程前遇到軟件問題，因而須把預定完成日期推延。有關設置中央檔案伺服器、提供安全電子郵件設備，以及強制對端點流動裝置進行加密的工作，預計在二零一零至一一年度完成。

醫院管理局

二零一零年六月

附件 **2**

二零零九年七月至二零一零年六月

政府資料泄漏事故摘要

項目	事故日期	局／部門	事故摘要和跟進措施
1	2009年8月	政府統計處	遺失一個載有保密資料的抽取式硬碟。所涉及的資料不屬敏感資料，因爲稅務局轄下的商業登記署可應市民要求提供有關資料。當中並無涉及個人資料。統計處已忠告有關員工在處理保密資料時，必須遵守保安指引。
2	2009年10月	勞工及福利局	遺失一枚便攜式儲存裝置，內載有曾參與理工大學一項研究計劃的 2 666 名參與者的個人資料。勞工及福利局認爲有關資料並無外泄，因爲該裝置在校園內遺失後不久便尋回。勞工及福利局已通知所有受影響人士，並已知會個人資料私隱專員。隨後亦實施一連串強化資料傳送和儲存的措施。該名肇事大學員工事後已辭職。
3	2009年12月	大學教育資助委員會秘書處(下稱“教資會秘書處”)	一個網上應用系統的其中一項預覽功能錯誤地使系統用戶的個人資料被一小撮其他人士在無意中看到。該程式錯誤是由教資會秘書處的資訊科技承辦商所引致的。教資會秘書處已知會個人資料私隱專員，並向六名受影響人士致歉。教資會秘書處其後已找出並糾正該網上應用系統的程式錯誤。紀律處分並不適用於本個案。
4	2009年12月	警務處	警務處超過 100 份由 2002 年至 2008 年的文件，經 Foxy 軟件在互聯網上被發現。有關資料涉及 118 名員工和 83 名市民的個人資料。警務處已通知受影響人士，並已知會個

項目	事故日期	局／部門	事故摘要和跟進措施
			人資料私隱專員。對有關人員所作的紀律覆檢已完成或在進行中。
5	2010年2月	衞生署	遺失一枚私人擁有的便攜式儲存裝置，內載有三名人士個人資料，包括姓名和身份證號碼。衞生署已通知所有受影響人士，並已口頭知會個人資料私隱專員。肇事員工已遭受口頭警告。
6	2010年4月	康樂及文化事務署(下稱“康文署”)	在一宗爆竊案中，一台載有 410 名人士(員工及其家人)個人資料的辦公室電腦被偷去。有關的電腦設有用戶名稱和密碼保護，而載有個人資料的檔案，則設有存取控制措施。康文署已知會個人資料私隱專員，並已通知所有受影響人士。紀律處分並不適用於本個案。
7	2010年4月	教育局	一部放於已上鎖辦公室內的個人電腦，懷疑被未經授權使用。所有儲存於其中一個磁碟機的資料發現被刪除。在一些被刪除的檔案中，載有大約 20 人的個人資料。教育局已向警方報案並知會個人資料私隱專員。待警方調查後，才決定是否通知受影響人士及會否需要有紀律處分。
8	2010年6月	創新科技署	創新及科技基金下的創新及科技支援計劃的一名評審委員遺失一張光碟，內載有向支援計劃申請撥款的申請項目資料，以及九名項目成員的個人資料。有關的光碟設有密碼保護，而所有資料亦已加密。創新科技署已知會個人資料私隱專員，並已通知所有受影響人士。該評審委員亦已就遺失光碟一事報警。紀律處分並不適用於本個案。