二零零九年七月十三日

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

本文件旨在告知委員自上次二零零八年十二月匯報至今，政府在推行各項資訊保安改善計劃方面的進展。

背景

2. 在二零零八年十二月八日舉行的資訊科技及廣播事務委員會(下稱“委員會”)會議上，我們向委員闡述政府在推行各項資訊保安改善計劃的進展。這些計劃的目的，是加強保護個人和敏感資料，以及確保政府決策局／部門(下稱“各局／部門”)遵行《個人資料(私隱)條例》(第 486 章)的規定，採取所有可行措施，以防在未經授權的情況下披露個人資料。委員要求政府在六個月後，就現有和擬採取的保安

改善措施，再次向委員會匯報有關進展。

3. 政府非常重視保護個人和敏感資料。有關改善措施包括爲處理問題而作出的修正，以及一連串由當局統籌的工作，藉以保障資訊安全、加強保護個人資料，以及減低再次資料泄漏的風險。

資訊保安改善計劃的進展

4. 改善計劃涵蓋四個主要範疇，即員工的資訊保安認知和教育、技術和程序措施、遵行保安規定審查，以及保安規例、政策和指引檢討。下文載述各範疇的工作進展：

(i) 員工的資訊保安認知和教育

5. 資訊保安認知和教育，是影響員工在工作間行爲表現的主要因素。政府旨在協助員工培養和維持高水平的資訊保安意識，從而提升各局／部門的整體資訊保安狀況。

6. 我們已於二零零九年年初改善計劃推出時，向員工進

行調查，從他們對資訊保安的態度、所具備有關的知識，以及遵行資訊保安規定等方面，了解他們現時的資訊保安認知水平。有關結果載於**附件 1**。概括而言，大部分員工均關注涉及資料保護的事故，並願意參與推廣或加強資訊保安的活動。

7. 在資訊保安認知方面，約 98%受訪員工認爲保護資料是重要的或非常重要的，這表示他們意識到須審慎和穩妥地處理資料。在對政府保安規定的認識方面，受訪員工之中，曾閱覽政府保安規例和資訊科技保安政策相關部分者，分別佔大約 90%和 77%。在作業模式方面，受訪員工均有遵行最佳作業模式指引，以保護其個人電腦和資料。受訪員工之中，約 80%已採取措施，利用密碼保護個人電腦，並慣常檢查打印機，確保沒有機密文件遺留在無人看管的打印機上。

8. 調查也顯示，曾閱覽保安規定的員工，在處理個人資料時，也會作出恰當的表現。

員工溝通計劃

9. 深固的資訊保安文化是需要時日培育的。自二零零九年年初起，政府資訊科技總監辦公室推出爲期一年的員工溝通計劃，以跟進員工調查的結果，並協助員工培養和維持高水平的資訊保安意識、汲取更多工作知識和培養良好習慣，並致力保護機密和個人資料。這項計劃旨在令員工重視和明白其所肩負的職責，是要保護交給他們保管的資料。

10. 我們已採用多種溝通工具和透過不同渠道，包括單張、海報、醒目提示、專題研討會、網上培訓課程、錄像培訓教材、員工通訊刊載的文章、主題網頁、遊戲、問答比賽、巡迴展覽和電子卡設計比賽，確保能有效地向不同的員工傳達訊息。

11. 二零零九年四月，超過 250 名來自各局／部門的管理和高級人員出席政府資訊科技總監辦公室舉辦的資訊保安會議。他們在會上分享經驗，講解在管理、營運和提供政府服務方面，有助停止資料泄漏的辦公室文化和作業模式。在會議上，政府資訊科技總監辦公室、保安局和公務員事務局的高級人員向與會者強調，並促請他們維護所屬局／部門的保安政策和措施，當中首要做的是採用適當保安機制，以及

協助員工認識和了解有關資料保安措施。

員工培訓

12. 我們致力爲員工提供持續不斷的培訓，以便爲他們提供最新資訊、和鞏固他們對資訊保安的了解和關注。在過去12 個月，我們已爲各局／部門逾 3,000 名員工舉辦超過 20 項課堂培訓課程和研討會。各類培訓活動的詳情，載於**附件 2**。這些課程部分包括導師培訓課程。我們已研製培訓資料套，協助各局／部門因應其部門目標、業務程序和營運環境，爲所屬員工提供更切合他們的培訓。

13. 政府資訊科技總監辦公室已聯同公務員事務局轄下的公務員培訓處，共同制訂靈活的教學方法，讓員工按個人進度修讀各類網上培訓課程。自本年四月至今，已有超過2,600 名員工報讀各項課程。此外，我們已安排由服務供應商提供培訓服務的常設合約，以推廣政府人員的保護資料意識。我們也已計劃在下半年舉辦更多有關個人私隱和資料保護的培訓課程和研討會。

(ii)　技術和程序措施

防止資料因使用點對點軟件和便攜式儲存裝置而泄漏

14.　二零零九年二月，我們向各局／部門發出“針對使用點對點軟件所產生風險而採取的資料保護措施”的通告，就如何防止可能發生的資料泄漏事故提供清晰指引，當中特別提及在辦公室以外的地方工作或使用安裝了點對點軟件的私人擁有電腦時須注意的事項。除了提醒員工切勿在私人擁有的電腦設施，包括便攜式儲存裝置，儲存或處理機密資料外，也建議他們定期檢查其電腦和儲存裝置(例如 USB 閃存盤、光碟、軟磁碟等)，和清理非故意地遺留在該等電腦或儲存裝置內作公務用途的個人或機密資料。上述措施務求盡量減低泄漏資料的風險。

技術工具和解決方案

15.　各局／部門正透過各種技術工具保護資料，當中最廣爲採用的是加密工具和解決方案。採取這些措施，可在遇到保安威脅或黑客入侵，又或遺失儲存媒體時，盡量減低泄漏

資料的風險。一些局／部門亦正計劃採用更先進的保安解決方案，以助管制 USB 裝置接駁至個人電腦。

16. 採用適當的技術工具和解決方案，有助員工防止資料泄漏。我們會繼續向各局／部門提供最新的技術資訊和解決方案，並會舉辦有關資料保護的技術研討會，內容涵蓋加密工具、端點保安解決方案和安全移除工具等。

(iii) 遵行保安規定審查

17. 由政府資訊科技總監辦公室統籌在各局／部門進行的獨立保安審計，已於二零零九年五月完成。整體結果顯示，各局／部門的資訊系統普遍符合政府的保安規定，而經確定有待改善的地方也正妥爲跟進及已採取改善措施。各局／部門的管理層已加緊注意及努力保護資料，並更着重加強員工培訓，以提高他們在遵行保安規例和政策方面的認知、知識和能力。各局／部門嚴禁員工在政府提供的電腦使用未經授權的軟件，尤其是點對點檔案共享軟件，並已採用適用的保安技術，包括加密儲存、數碼證書和虛擬專用網絡。大部分局／部門在進行部門保安風險評估方面，均顯示高水平

的表現。我們會於未來定期進行保安審計。

18. 我們已應委員於二零零八年十二月八日委員會會議上所提要求，提供有關香港警務處保安風險評估的資訊，有關詳情載於**附件 3**。跟據獨立保安審計的結果，警務處經審查的範疇均符合有關保安規定。儘管如此，審計師也就若干有待改善的地方提出建議，而警務處現正作出有關的改善措施。政府資訊科技總監辦公室會繼續與香港警務處跟進此事。

(iv) 檢討資訊保安規例、政策和指引

19. 政府已制訂有關保安的規例和政策，包括訂明須遵行《個人資料(私隱)條例》的規定。當局已強調，如保安事故涉及個人資料，有關的局／部門須盡快通知個人資料私隱專員，並盡可能知會受事故影響的人士。

20. 政府會定期檢討有關資訊科技保安的規例、政策和指引，確保與時並進，以配合科技的進步、國際的發展和業界的最佳作業模式。二零零九年一月，政府資訊科技總監辦公

室已展開有關檢討工作，以期在二零零九年年底前公布經修訂的規例、政策和指引。該檢討會參考資訊科技先進的國家的保安政策和相關的國際標準(例如國際標準化組織所公布的 ISO27001 和 ISO27002，以及資訊及相關技術的控制目標)，以釐訂本港的保安政策。我們會增添實用資料和案例，方便員工參考，使他們容易明白保安規定和作爲有效的日常運作。

政府的資訊保安狀況

21. 在二零零八年，政府資訊保安事故應變辦事處共接獲 19 宗保安事故[1]報告。該辦事處負責中央協調各局／部門，以處理政府資訊保安事故。在二零零九年的首兩季，辦事處共接獲十宗事故報告，當中有六宗是資料泄漏事故。其餘的四宗事故，都是關於政府網站受到惡意襲擊(如試圖入侵)或網站假冒。所有事故都很快被糾正，而部門內部系統並沒有受到影響。有關資料泄漏事故的摘要載於**附件 4**。雖然二零零九年年初仍有資料泄漏事故發生，但所造成的影響已大爲

[1] 須呈報的保安事故包括：未獲授權接達、拒絕資源、中斷服務、泄漏電子機密資料、惡意破壞或竄改數據／資料、滲入和入侵、電腦病毒和惡作劇電子郵件，以及影響網絡系統的惡意程式碼或手稿程式。

減少，因爲當局已採取保護措施，例如有關資料或遺失的儲存裝置已經過加密保護。有關的各局／部門已就該等個案通知個人資料私隱專員，並在適當情況下知會受事故影響的人士。各局／部門亦跟據既定程序，對違反了保安規例和程序的員工，採取了相關的跟進行動，包括紀律處分。

公眾的資訊保安

學生與教師

22. 政府繼續向市民推廣資訊保安，集中宣傳正確使用電腦設施的訊息，並教導他們如何保護電腦資源和資訊資產。學校探訪活動自二零零八年年初展開至今，我們已舉辦了 35 次學校探訪活動，有超過 9,000 人參與。學校探訪活動備受參加者歡迎，有助向所定對象傳遞網上安全的重要信息。鑑於反應良好，成效理想，我們會繼續進行這類學校探訪活動，爲師生和家長們舉辦講座和討論會，並就有關資訊保安的事宜，以及如何合乎行爲準則地使用資訊科技和互聯網服務，向他們提供意見。

23. 另外，政府推行一項爲期一年的全港互聯網教育活動，教導互聯網用戶，特別是年青學生如何正確和安全使用互聯網。這項活動旨在向年青學生強調，應重視和尊重個人資料私隱和知識產權，並應避免過分沉迷上網，以及防禦電腦病毒攻擊等。

商界企業

24. 近年來，殭屍網絡[2]日益威脅互聯網的穩健發展和網上安全。二零零九年四月，Conficker電腦蠕蟲[3]爲用戶帶來很大的安全威脅，不單令電腦受到感染，更把這些電腦變成大型全球性殭屍網絡的一份子。我們聯同香港電腦保安事故協調中心，密切監察Conficker蠕蟲的情況，並迅速通告電腦用戶有關最新進展和抵禦攻擊的方法。此外，政府資訊科技總監辦公室、警務處和香港電腦保安事故協調中心在二零零九年五月舉行了互聯網服務供應商研討會，組織各互聯網服務供應商，合力對付殭屍網絡，並提升香港作爲領先數碼城市

[2] 殭屍網絡是指被操縱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操縱，可被遠程操控在網上進行惡意活動。

[3] Conficker 是一種電腦蠕蟲，在二零零八年十月首次出現，之後不斷演變，相信全球數以百萬計的電腦曾受到感染。

的保安狀況。在該研討會上，我們向互聯網服務供應商講述殭屍網絡的威脅，以及其他影響正常運作的保安攻擊；和分享互聯網服務供應商、香港電腦保安事故協調中心和執法機關可如何攜手合作，打擊該等罪行，最終有利於整體經濟發展。

25. 政府十分支持私營機構或保安組織爲市民舉辦的保安推廣活動。在過去 12 個月，政府資訊科技總監辦公室的高級人員曾出席六個在本地舉行有規模的保安會議，並在會上發表講話，向市民傳遞資訊保安的訊息和提供有關意見。

26. 我們會在二零零九年推行第五屆“全城電腦清潔日”活動。本屆活動的主題是電子交易的資訊保安。這項一年一度的活動旨在提高市民的資訊保安意識，以期他們加強保護電腦免受網絡攻擊。我們另會在八月和十一月，特別爲公共機構和中小型企業舉辦一連串研討會。

公共機構

27. 我們定期建議各局／部門與公共機構分享有關資訊

保安的政策、指引和技術資訊，以協助他們提升保安狀況。在近期二零零九年三月向各局／部門發出有關防禦Conficker蠕蟲的保安提示中，我們亦再次提醒他們對其轄下的公共機構和規管機構作出通告。政府資訊科技總監辦公室會繼續與各局／部門保持緊密聯繫，並協助他們向公共機構提供有關資訊保安事宜的意見和協助。

28. 醫院管理局就加強資訊保安和緩解資料泄漏風險，繼續採取需要的措施，有關他們進展的摘要請參閱**附件 5**。

總結和未來路向

29. 政府與所有其他企業一樣，無可避免地也面對各類資訊保安的風險，包括資料泄漏。世界各地的機構組織，均廣泛出現違反保安規定的情況，只有少數能倖免。我們會堅決執行資訊保安政策和有關作業模式，並會採取措施，以進一步加強市民對我們管理其個人和敏感資料方面工作的信任。

30. 要解決所有保安問題，並非一朝一夕便可辦到，而且現時也沒有一勞永逸的解決方法。我們會繼續採取多管齊下

的方法，採用不同措施和進行多項工作，以應付政府在資訊保安方面的各種要求，並在需要時更新有關工作內容。我們當前的目標是培育濃厚的保安文化，讓每名員工都明白，他們的積極參與，對防止資料泄漏至爲重要。這種文化需要時日培育和紮根。我們建議在一年後向委員會匯報各項保安措施的進展，讓委員備悉有關情況。

徵詢意見

31. 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

二零零九年七月

附件 **1**

資訊科技及廣播事務委員會二零零九年七月十三日會議

二零零九年一月進行的員工資訊保安認知初步調查

由於資訊保安認知是無形的，因此難以直接作出衡量。這項有關員工的初步調查在二零零九年年初進行，旨在評估一些涉及員工保安認知和教育的因素。受訪者的回應經分析後，可助反映員工的資訊保安認知(他們的看法)、他們的資訊保安知識(他們所知道的)，以及他們的行爲習性／所作出的努力(他們所做的)等方面的情況。

2. 在資訊保安認知方面，調查結果顯示，現時大部分員工均察覺到資料保護的問題。**圖1**顯示約98%受訪員工認爲資料保護是重要的(22%)或非常重要的(76%)，這表示他們意識到需要審慎和穩妥地處理資料。員工體會到資訊保安的重要性，因此會更爲注意須穩妥地處理資料，爲推動資訊保安文化踏出第一步。我們須透過不同途徑舉辦推廣活動，以繼續推動這股風氣。

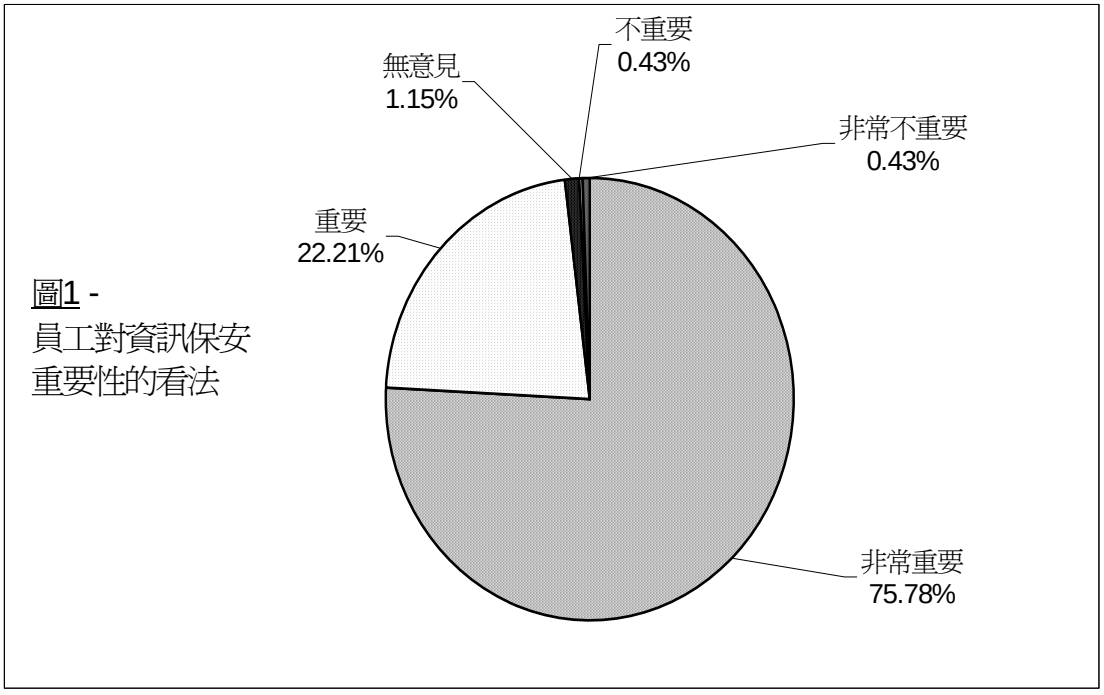


圖1 -
員工對資訊保安
重要性的看法

3. 在資訊保安知識方面，調查結果顯示，員工可加強熟習政府保安規例和資訊科技保安政策。**圖2和圖3**分別顯示約90%受訪員工曾閱覽保安規例(有些只選閱部分)，77%曾閱覽資訊科技保安政策(有些只選閱部分)。調查結果也顯示，擁有較豐富知識的員工，在保護資料方面一般也展示較佳的行爲表現。

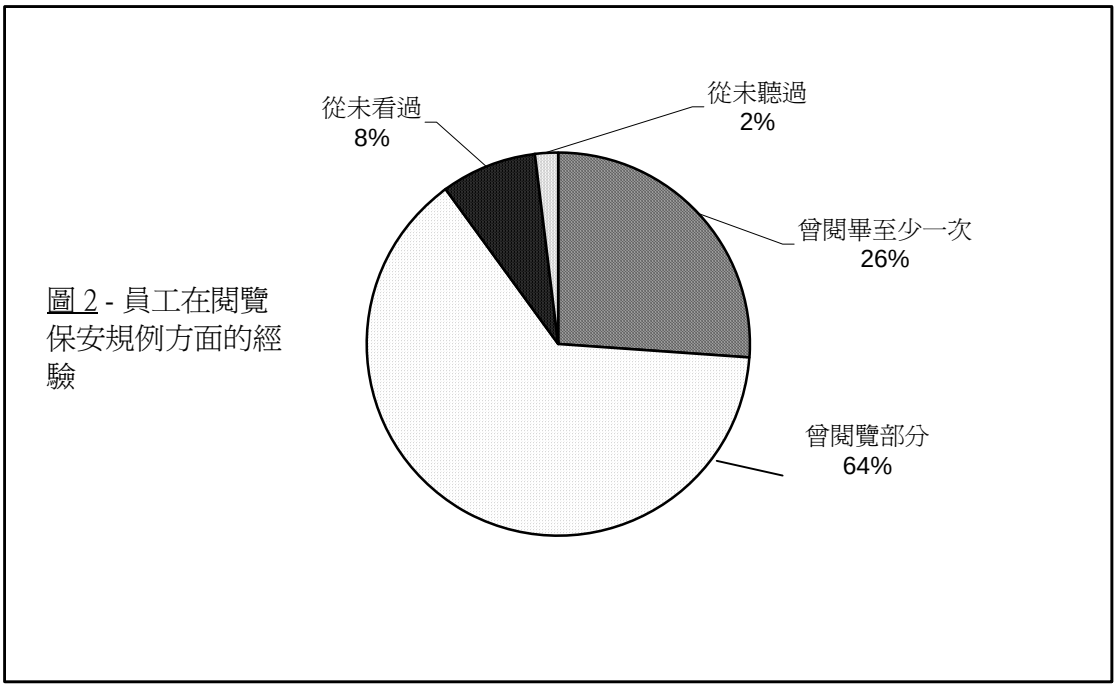


圖 2 - 員工在閱覽保安規例方面的經驗

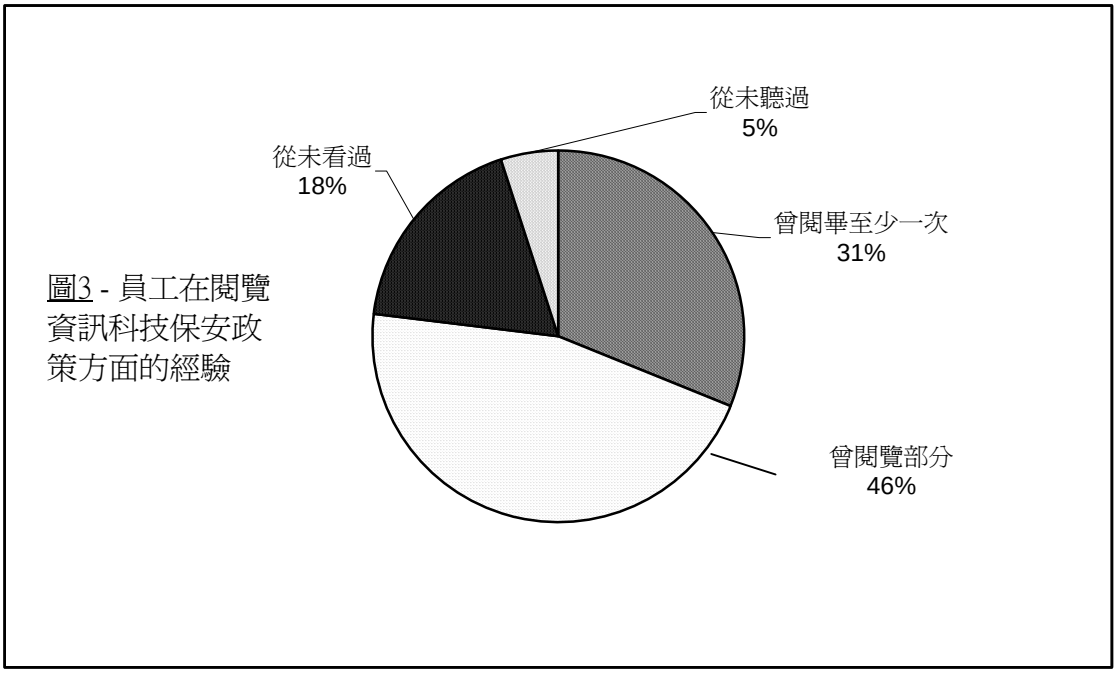


圖3 - 員工在閱覽資訊科技保安政策方面的經驗

4. 在日常運作方面，員工一般都會遵守指引，保護其個人電腦，並採取適當措施保護資料。調查包括數條有關員工採取保安措施的問題，藉以反映他們的行爲習性，從而推

論他們在資訊保安方面所作出的努力。**圖4**顯示，近80%受訪員工在離開電腦前，經常或很常啓動屏幕保護程式密碼。同樣，一如**圖5**所示，近80%受訪員工會經常檢查是否有任何載有機密資料的打印本遺留在無人看管的打印機上。

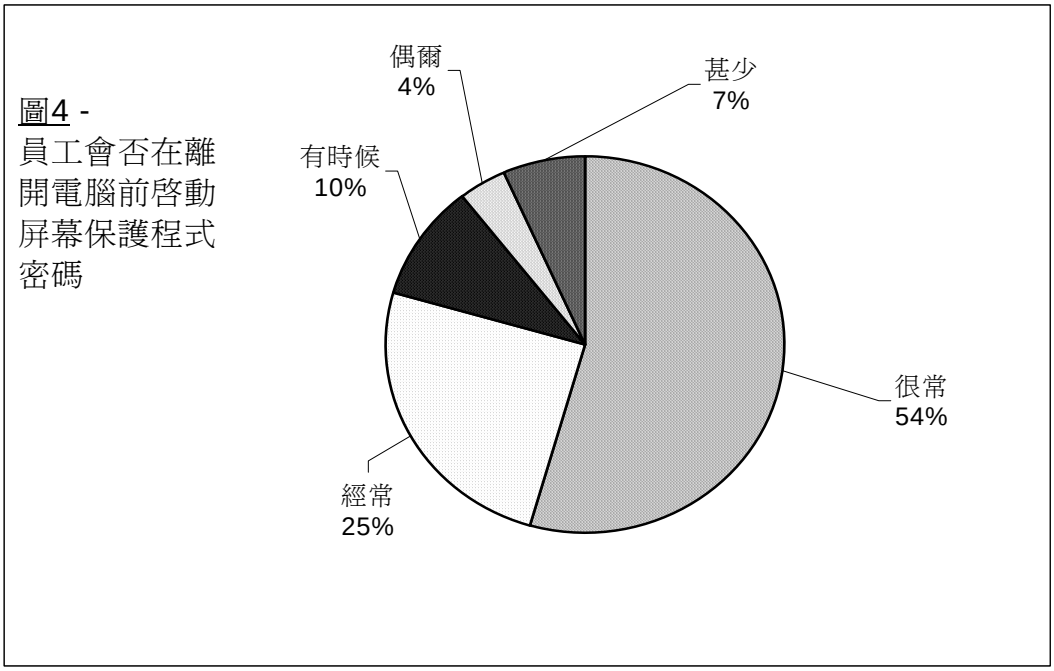


圖4 - 員工會否在離開電腦前啓動屏幕保護程式密碼

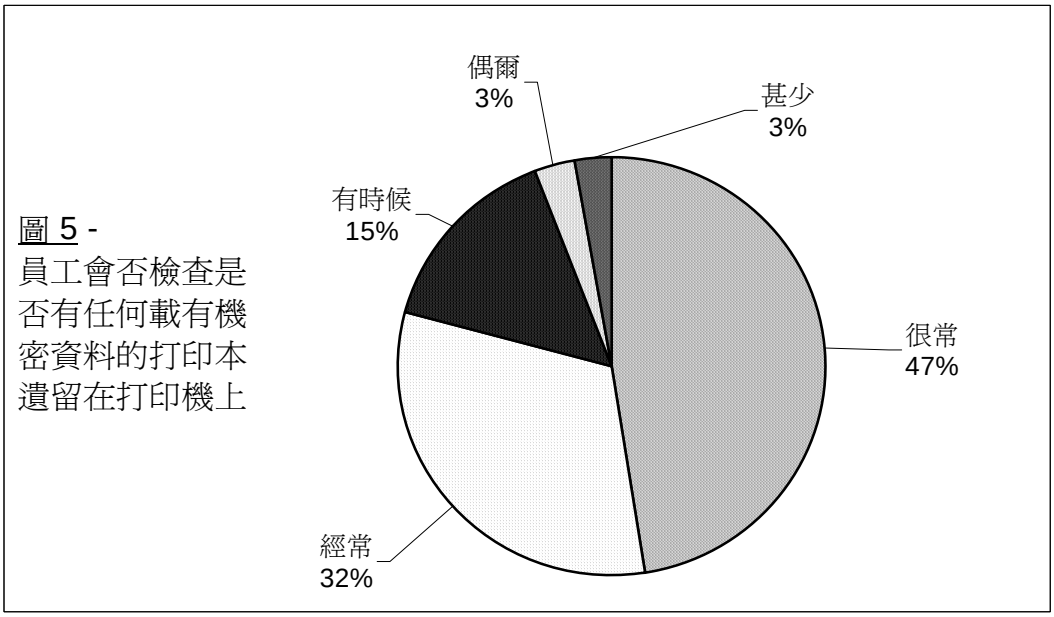


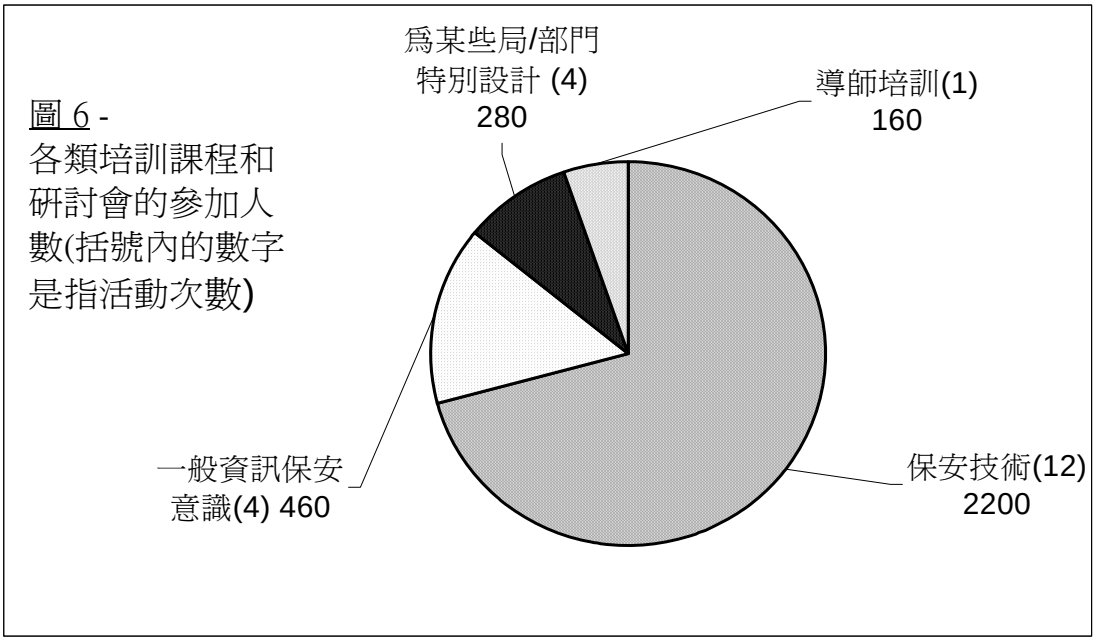
圖 5 - 員工會否檢查是否有任何載有機密資料的打印本遺留在打印機上

附件 2

資訊科技及廣播事務委員會二零零九年七月十三日會議

二零零八年六月至二零零九年五月舉辦的

資訊保安培訓課程、研討會和有關活動



在過去 12 個月，我們曾爲各局／部門逾 3 000 名員工舉辦或協辦超過 20 次課堂培訓活動和研討會。

附件 3

資訊科技及廣播事務委員會二零零九年七月十三日會議

香港警務處的保安風險評估

政府已完成涵蓋各局／部門的保安審計，以便獨立評估各局／部門遵行保安規定的情況。在政府資訊科技總監辦公室統籌下，獨立審計師已於二零零八年十二月至二零零九年五月其間，爲香港警務處(警務處)進行保安審計。下文扼要闡述該項審計工作的成效和結果。

2. 審計結果顯示，警務處已按照有關保安規定，妥善推行保安措施，以保護警務處的資料和系統。警務處符合所有審查範疇訂下的保安規定，這些範疇包括資訊科技服務外判保安、設備保安、系統接達和儲存保安、資料保安，以及網絡和通訊保安。

3. 審計師曾造訪有關人員，並檢視警務處的保安政策、程序和設置，另又檢察證明文件如報告、表格和電子郵件，實地視察數據中心和電腦室，以及抽樣審查選定的重要系

統。

4. 在使用便攜式電子儲存裝置方面，審計師認爲，警務處已執行嚴緊的管制措施。根據部門政策，所有用以儲存機密／個人資料的便攜式電子儲存裝置，均須由部門提供。至於所有私人便攜式電子儲存裝置，則一律禁止使用。

5. 爲防止因使用配置錯誤的軟件而導致意外泄漏資料，警務處禁止安裝任何未獲授權的軟件。在執行日常業務工作時，警務處並無使用點對點檔案共享軟件。

6. 該項審計也就警務處定期進行的保安風險評估，審研有關程序和成效。警務處在評估前和評估期間所進行的工作，以及在撰寫評估報告和採取跟進行動等方面，都獲取正面的評核。警務處在進行保安風險評估時，一直緊遵政府資訊科技總監辦公室所發出的規定。

7. 警務處多個重要系統被選作進一步仔細研究。這些系統的保安風險處於合理的低水平。在這次審計中沒有發現新的風險，而審計師只建議警務處在若干方面作出改善，特別

是：

- 加強管制定期或抽樣查察操作記錄；
- 加強現有的資訊科技資產清單管理；以及
- 研究制訂全面的方法，以減少把機密資料帶離辦公室的需要。

8. 儘管警務處已遵行有關規定，但在二零零九年年初仍發生一些資料泄漏事故，而有關原因可能是涉及的人員資訊保安意識不足。爲減低員工缺乏資訊保安認知而可能引致的風險，警務處已定期爲員工舉辦內部培訓活動／簡介會、外間培訓活動／簡介會、網上學習課程，並定期向他們發出有關提示，使他們知道保護機密和個人資料的重要性。該處也爲各級員工舉辦資訊保安認知培訓課程，包括處理個人私隱資料培訓、資訊保安培訓和導師培訓計劃。

9. 政府資訊科技總監辦公室會與警務處一起跟進審計師所建議須作出改善的地方。一如政府保安政策所規定，警務處會定期安排獨立審計師，就該處的應用程式和系統進行保安風險評估，確保這些應用程式和系統符合嚴格的保安要求。

附件 4

資訊科技及廣播事務委員會二零零九年七月十三日會議

二零零九年首兩季政府資料泄漏事件的摘要

項目	事件日期	部門	事件摘要和跟進措施
1	2009 年 1 月	食物環境衞生署	一枚屬於食物環境衞生署員工的便攜式儲存裝置，被發現遺留在公共巴士上。便攜式儲存裝置內存有未完成撰寫的文件和涉及 103 名市民的個人資料。食物環境衞生署事後已通知有關的市民，並向他們道歉。事件亦已知會個人資料私隱專員。
2	2009 年 1 月	香港警務處	香港警務處遺失了一枚由處方提供的便攜式儲存裝置，內存有一些內部的資料和涉及 26 名市民的個人資料。儲存的資料已受設有堅固的密碼及 AES 256-bit 加密技術以防止裝置內的資料被讀取。
3	2009 年 2 月	食物環境衞生署	一些涉及食物環境衞生署員工的評核資料，通過 FOXY 軟件在互聯網上被發現。署方確定泄漏的資料，是一份屬於一名非公務員合約僱員未完成的評核報告，並已向該僱員致歉。由於被披露的資料只有受評人和評核人的姓名及職位，而並不包含其他個人資料，署方沒有知會個人資料私

項目	事件日期	部門	事件摘要和跟進措施
			隱專員。
4	2009 年 2 月	香港消防處	一些香港消防處的文件，包括 32 名員工的評核報告及內部資料，通過 FOXY 軟件在互聯網上被發現。當中涉及 58 名香港消防處員工的個人資料。香港消防處已通知所有受影響人士，並已知會個人資料私隱專員。
5	2009 年 2 月	香港警務處	一些香港警務處內部資料，通過 FOXY 軟件在互聯網上被發現。這些資料是一個用作撰寫街頭賭博個案口供的範本檔案，並不牽涉個人資料或任何個案資料。
6	2009 年 3 月	香港警務處	香港警務處一些由 2004 年至 2008 年的內部文件，通過 FOXY 軟件在互聯網上被發現。這些資料包括 60 名員工及 36 名市民的個人資料。香港警務處已在可行情況下通知受影響人士，並已知會個人資料私隱專員。

附件 5

資訊科技及廣播事務委員會二零零九年七月十三日會議

有關醫院管理局所採取的行動的進展

目的

本文件旨在向委員闡述自二零零八年十二月八日委員會會議後，醫院管理局（醫管局）就有關二零零八年的遺失病人資料事件所採取的行動和所取得的進展，以及調查結果和建議，以加強病人資料安全及私隱。

背景

2. 醫管局專責小組及個人資料私隱專員分別就八個範疇提出了 26 及 37 項建議，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。隨後，醫管局訂下了相應的行動和計劃以回應這些建議，並會在 18 個月內完成所有相關的工作。

行動計劃及進展

3. 醫管局大會於二零零八年九月十日的內務會議上，獲悉專責小組和私隱專員報告的結果和建議，並批准醫管局就這些建議擬採取的行動計劃，以進一步加強保障病人資料安全及私隱。該行動計劃涉及 19 個綜合目標，並涵蓋上文第 2 段提及的八個範疇。

4. 以下是已採取的主要行動撮要：-

(a) 醫管局與個人資料私隱專員合作，爲所有醫管局員工舉辦加強私隱意識運動，透過研討會和直接討論，培訓醫管局人員，該運動並已經於二零零九年五月啓動。 爲確保醫管局員工於《個人資料(私隱)條例》，政策和實際工作上得到適當的培訓，以保護病人的個人資料，醫管局已製作其他教育項目，包括網上學習教材；

(b) 醫管局已委任機構資訊保安及私隱主任出掌新成立的醫管局資訊保安及私隱辦事處、以及監督醫管局所有相關的資訊保安及私隱措施；

(c) 醫管局總辦事處及聯網資訊保安及私隱委員會現已成立，該委員會已全面運作，以監督所有行動計劃的改善

措施；

(d) 已檢討全醫管局適用的資訊保安及私隱政策，並通報及發放給所有醫管局員工，讓他們明白資訊保安及私隱的原則和重要性；

(e) 已制訂聯網資訊保安及私隱的執行監察要求，並加強外判合約條款上資訊保安及私隱相關要求；

(f) 已檢討及減少主要資訊科技系統內可以下載病人資料的用戶數目；

(g) 已加強個人電腦安全以杜絕資料外泄，減少病人資料下載並將資料加密。

5. 餘下的行動計劃目標包括政策和指引的檢視，措施執行的查核和其他科技改善措施預料可逐步於二零一零年第一季度完成。

醫院管理局

二零零九年六月