地 產 代 理 監 管 局
ESTATE AGENTS AUTHORITY

地產代理資訊保安及私隱保護政策與指引

目錄

1 目的

隨著資訊系統及數碼化設備的使用日益增多，保護個人資料私隱變得愈見重要及複雜。本文件旨在向地產代理及其僱員介紹保護個人資料私隱的最低要求。

本文件所載之政策乃供所有地產代理及其僱員參考而製訂。地產代理應注意，本文件所載之政策闡述明確的監管要求，地產代理及其業務夥伴應予以遵守。本政策使地產代理可在適當的情況下實施特定的控制及保護措施。

有關資訊系統技術要求的標準及指引的具體建議，請參閱本文件附錄中兩份分別關於小型代理[1]及中及大型代理的指引。

本文件並非全面的政策範例，亦不影響地產代理監管局根據《地產代理條例》行使其監管職能及權力。

[1] 就本文件而言，小型代理是指擁有 4 間或不足 4 間辦事處的代理，而中及大型代理是指擁有 5 間或更多辦事處的代理。

2 定義及慣用詞

2.1 定義

1. 可用性	資訊系統應在任何既定或指定的時段內供使用者使用。
2. 電腦室	放置主要電腦設備的專用房間。
3. 機密性	由資訊系統儲存或處理而僅供獲授權人士知悉或查閱。
4. 承辦商／次承辦商	由直接或透過另一間公司提供服務的公司所僱用的人士，而不論僱用的期間及條款如何。
5. 資料當事人	就個人資料而言，指屬該等資料當事人的個人。
6. 資料使用者	就個人資料而言，指獨自或聯同其他人或與其他人共同控制該等資料的收集、持有、處理或使用權的人士。
7. 指引	推薦的有效保安實務，應在可能的情況下實施。
8. 資訊	呈現事實、概念或指示並可由人工或以自動化方式進行通訊、解釋或處理的一種具體形式。資訊以對話口頭通訊、文書或電腦網絡等多種方式傳播。資訊亦以多種格式存取，包括但不限於：電腦資料庫或傳輸、磁帶、軟磁碟、電腦製成的報告、書面文件、電郵訊息、話音郵件、會議記錄及工作底稿。
9. 資訊保安	從發送者到接收者或從客戶端到伺服器的資訊資產保護。資訊保護通常指保護資料的「機密性」、「完整性」及「可用性」。保安應被視爲促進而非阻礙業務的方法。
10. 資訊系統	透過使用資訊科技以電子方式處理資料的電子資訊系統，包括但不限於：電腦系統、伺服器、工作台、終端機、儲存媒體、通訊設備及網絡資源。
11. 資訊使用者	因公務需要而在在線或離線的情況下檢閱、取閱或使用資訊系統中的資料或資訊的人士。
12. 完整性	僅獲授權人士才獲許可更改資訊系統內已儲存或處理的任何方面的資訊。
13. 僱員	受僱人士 (不論僱用期間及條款)。凡符合文意，僱員亦包含服務承辦商之僱員。

14. 標準	指明適當使用電腦資源，作爲一種保安政策控制措施的強制行爲模式。
15. 系統管理者	負責系統及網絡資源每日運作的人士。
16. 系統使用者	在履行職責的過程中，負責在資訊系統中輸入或檢索當時所需資料或資訊的人士。

2.2 慣用詞

以下乃本政策中的慣用詞列表：

須	使用「須」字即表明此乃強制性要求。
應	使用「應」字即表明此乃良好實務的要求，應在可行的情況下實施。
可	使用「可」字即表明此乃適宜的要求。

3 控制及監管查閱資料權限：須知

3.1 管理層

3.1.1 保護客戶的個人資料乃每位僱員之責任。高級管理層或執行其職務的人須教導其僱員遵守本政策，並加強僱員對個人資料私隱保護的意識。

3.1.2 在分配資訊系統資源及權限予使用者時，須以最小權限爲原則。

3.1.3 客戶的個人資料不得向外部人員或承辦商披露。如必需披露該等資料，則須採取防範措施。

3.1.4 須確保在控制範圍內 (包括已外判系統) 的資訊的機密性、完整性及可用性，以及資訊系統的所有其他方面的保安。

3.1.5 應明確界定每一特定層級僱員在資料私隱及保護方面的角色及責任。

3.1.6 應定期對資料保護進行資訊保安審核。

4 系統完整性

4.1 識別使用者

4.1.1 資訊系統的每名使用者在接入系統時，須有其自己的使用者身份。亦應定期復核其使用系統的權限。

4.1.2 使用者需對以其身份執行的所有活動負責。

4.1.3 應界定嚴格的密碼政策，而政策最少包括：最小的密碼長度、初始設定、禁用字母及格式、密碼使用週期，亦應包括合適的系統及使用者密碼選擇指引。

4.2 系統保安

4.2.1 須在儲存敏感個人資料的伺服器或電腦上安裝反惡意軟件。

4.2.2 應定期備份個人資料，以防資料遭意外刪除或破壞。

4.3 實體設備保安

4.3.1 所有資訊系統須置於安全環境中或交由僱員看管，以防被未經授權查閱。

4.3.2 僱員應注意及採取高度防護措施，以保護公司提供予他們的電腦設備。

4.3.3 須妥善保護資料中心、電腦室或重要系統 / 電腦的存放區，並對進入該等區域予以嚴格控制。

5 資料及資訊使用的規限及監控

5.1 概述

5.1.1 須明確界定查閱資料的權限，並由管理人員定期復核，且該等權限應只授予有需要查閱該等資料的人士。

5.1.2 應採用正式的授權程序，對敏感個人資料的所有查閱皆須記錄在案，以作爲控制查閱權限分配的措施。

5.1.3 當使用者離開其工作台時，應啓動預防措施以防敏感資訊被未經授權查閱。

5.1.4 僱員不應從辦公室複制及帶走公務資料及 / 或將其下載至家庭或個人電腦設備上。如必須複製 / 下載該等資料，則須事先取得高級管理層的批准。

5.1.5 管理層應確保第三者服務供應商注意並遵從本政策及有關當局發佈的其他資訊保安要求。

5.1.6 應採取合理的保安措施 (如防火牆、反惡意軟件 / 防毒軟件及 / 或入侵檢測機制) 以保護公司網絡的接入。

5.1.7 除獲高級管理層批准，嚴格禁止將私人擁有的電腦設備 (包括個人的筆記簿型電腦、電子手賬 (PDA)、通用串列匯流排 (USB) 等存儲設備等) 連接至公司網絡。

5.2 私隱

5.2.1 管理層應保留檢查所有在資訊系統中儲存或傳輸資訊的權利，以確保資訊符合《個人資料 (私隱) 條例》的要求。

5.2.2 應遵循所有相關規例中就使用敏感資料的要求。收集及保存的個人資料須：

- 僅可用於收集資料時述明的用途；
- 在法律或規例規定的時間內予以保存，或者按所需要的時間予以保存，而不得超過必要的時間；
- 遵照有關法律要求及棄置資料指引建議而刪除資料；及
- 在未經資料當事人明確同意前，不得披露資料。

5.3 記錄

5.3.1 高級管理層須確保就充份記錄資訊系統 / 應用程式的活動進行規範。

5.3.2 須在記錄具有審計效用的時期內保存該記錄。在此期間應妥善保管該等記錄，且僅供獲授權人士查閱。

5.3.3 記錄不得用於呈現某一個別使用者的活動，除非該查閱行爲是獲高級管理層指示的必要的審查活動。個別系統中的記錄僅可用於檢驗是否已遵守接入控制政策及已實施控制措施。該等記錄不得用以呈現使用者的活動，除非涉及個別審查或事件調查活動。

6 僱員培訓及意識

6.1.1 應在可能的情況下，就個人資料私隱及保護以及最新的資訊保安趨勢，向僱員提供定期的資訊講座或培訓課程。

6.1.2 須定期向僱員提供有關私隱及個人資料保護的內部備忘及通函，確保他們對當前資訊威脅有所警覺，並知曉如何在工作過程中遵守本政策。

- 完 -

附錄 A — 小型代理指引

目的

本指引旨在爲擁有 4 間或不足 4 間辦事處的地產代理提供更多具體意見，建議如何遵守《地產代理資訊保安及私隱保護政策》(下稱《政策》)。

本文所述指引並非強制性規定，而應被視爲合規技術標準的參考。地產代理應注意，本指引僅爲建議，他們應自行制定關於資料私隱及保護的規定。地產代理實施的保安措施水平亦應與可承擔的風險及可用資源的水平相稱。但地產代理實施的技術保護不得低於《政策》中列明的水平。

查閱資料的管理控制

1. 應提供必要資源，以主動支援資料私隱保護及資訊保安的措施。
2. 系統管理員接入包含個人資料的應用程式的權限應與一般使用者的權限分開；負責維修及保養電腦系統的資訊科技專責僱員或承辦商不得接入敏感個人資料。
3. 須確保應用程式系統及其資料的整體保安，防止資料洩漏或被未經授權披露。
4. 應定期發布提醒僱員有關下列事項的備忘錄：
   - 最新的資訊科技保安威脅及其防範措施；
   - 有關個人資料私隱法律及相關規定；及
   - 個人資料私隱及保護的內部控制及要求。
5. 應使用外部資源，定期對資訊科技系統的保安進行評估。

系統保安及保護

6. 對於每個應用程式，每位使用者僅可擁有一個使用者身份；不應支持共用密碼。
7. 當一名僱員因解僱、辭職或永久調識時，應盡快註銷或鎖定其使用者身份。
8. 使用者密碼至少爲六位，且由字母和數字組成，並密碼應每半年變更一次。
9. 使用者須牢記密碼，並不將密碼寫下在辦公室的任何地方。
10. 如安裝新的電腦設備，則須在任何資訊系統運作前，更改供應商提供 / 預設的密碼。
11. 伺服器或電腦上應安裝反惡意軟件 / 防毒軟件，該等軟件應每日自動更新惡意軟件 / 病毒的定義及掃描引擎 (scan engine) 。

12. 不應爲提高系統性能而關閉反惡意軟件 / 防毒軟件。
13. 定期備份所有個人資料。
14. 如需在國內或海外 (如酒店等) 進行遙距接入，則應使用適當的網絡保安技術 (例如虛擬網絡連線 (VPN) 或保密插口層 (SSL) 等)。
15. 如辦公室無人值守，則應鎖上主機設備所存放的地方。
16. 僱員應妥善保護分配予他們或由他們保管的電腦設備，如座枱式及便攜式電腦、可移動電腦設備或通用串列匯流排 (USB) 等儲存裝置；僱員不得任由電腦設備無人看管，除非該設備在已上鎖的環境受保護。
17. 外判承辦商應在地產代理僱員在場時履行其工作；不應因服務的需要帶走電腦設備。

資料及資訊使用的規管及監控

概述

18. 應在謹慎考慮後才分派查閱資料的權限予僱員。
19. 應安裝螢幕保護程式密碼及定向螢幕過濾器，以防敏感資料被未經授權查閱 / 讀取。
20. 應在已上鎖的環境下妥善保護備份媒體；不應使用個人儲存設備備份公務資料。
21. 由互聯網下載的所有軟件和檔案須經防毒軟件掃描檢驗。
22. 不得把敏感個人資料透過互聯網以電郵發送。
23. 在未獲高級管理層事先批准前，僱員不應在工作時間於公司的工作台使用私人互聯網電郵服務，尤其是以該服務發送個人資料。
24. 須安全地棄置不再使用的備份媒體及電腦 (如透過焚化、壓碎或消磁)。
25. 如使用者長時間離開工作台 (如午膳、會議等)，則應登出載有敏感個人資料的應用程式 / 系統。
26. 應定期復核其資料私隱及保護機制的有效性。
27. 應記下系統的使用記錄，以備將來有需要時進行保安復核。以下是應被記錄的建議項目：
    - 使用者身份；
    - 登入、登出及其他重要事項 (如使用主管賬戶) 的日期及次數；
    - 獲分配的接入權的任何變動；使用者賬戶及密碼的更改；
    - 系統設置、已安裝軟件及系統互連的任何更改；及
    - 接入系統時，成功及被拒的記錄。
28. 須嚴格限制查閱記錄檔案；系統及應用程式的審計記錄應至少保存六個月。

第三者接入

29. 承辦商或次承辦商的所有僱員應遵守適用於地產代理僱員的相同資訊保安及資料私隱的規定。他們應知悉，若違反《政策》及相關保安指引及標準，可能導致違反規定並引致法律訴訟。

30. 須在合約上界定或制定適用於第三者的保安規定。該等規定須輔之以供應商 / 承辦商 / 次承辦商的建議，但不得以任何形式降低或損害規定的保安水平。須針對所有供應商、承辦商及次承辦商撰寫及實行標準安全條款，以應對各具體情況。

31. 除地產代理明確批准外，承辦商或次承辦商不得查閱個人資料。

- 完 -

附錄 B — 中及大型代理指引

目的

本文件旨在爲擁有 5 間或更多辦事處的地產代理提供技術意見，建議如何遵守地產代理資訊保安及私隱保護《地產代理資訊保安及私隱保護政策》(下稱《政策》)。

本文所述的指引並非強制性規定，而應視爲合規技術標準的參考。地產代理應注意，本指引僅爲建議，他們應自行制定關於資料私隱及保護的規定。地產代理實施的保安措施水平亦應與可承擔的風險及可用資源的水平相稱。但地產代理實施的技術保護不得低於《政策》中列明的水平。

控制及監管接入的權限：須知

管理層

1. 管理層應提供必需的資源，以支援對僱員的資料私隱保護及資訊保安的教育及培訓課程。
2. 爲避免利益衝突，須明確界定並執行載有敏感個人資料的資訊科技系統的使用者及行政人員的適當責任分離。
3. 管理層應按只賦予有需要人士權限的基礎爲原則以賦予權限給各使用者 (內部或外部僱員) 。亦應定期復核該權限是否一致及符合執行的目的。
4. 應分隔負責資訊科技的僱員或承辦商在處理資訊系統時的職責，以避免利益衝突。
5. 管理層須確保在其控制範圍內 (包括已外判的系統) 的資訊的機密性、完整性及可用性，以及資訊系統的所有其他方面的保安狀況。
6. 若外部人員或承辦商在其服務期間需接觸客戶的個人資料，應要求其簽署保密協議。
7. 應每兩年 (或大概兩年) 由內部或外部核數師對資訊科技系統及基建設施進行一次資訊科技安全風險評估及審查，以確保其完整性及機密性。

系統完整性

使用者識別

8. 一個使用者身份只可用作識別一名使用者。不鼓勵共用或團體共用使用者身份，除非經管理層明確批准及已實行並記錄正式的認可程序。
9. 應在共用密碼的建立及使用過程中採用嚴謹的應用程序。僅在必需的情況下使用共用使用者身份及密碼，且須在每次使用後更改密碼。
10. 每半年或於僱員職位有所變動時復核使用者的系統權限。

11. 當一名僱員因解僱、辭職或永久調職，應盡快註銷或鎖定其使用者身份。
12. 使用者密碼至少爲六位，且由字母和數字組成，並應每半年更改一次。如應用系統有自動更改密碼的提示功能，則應啓動該選項。
13. 除非必須共用密碼 (如求助台支援、共用電腦及共用檔案)，否則不得共用或披露密碼，但如必須共用密碼，亦須獲得高級管理層的明確批准。
14. 在儲存或經由網絡發送密碼時 (在可能的情況下)，務必審慎保護密碼。若無法加密，則須應用補償性控制將資訊系統所面臨的風險降至可接受水平。
15. 禁止僱員獲取或以其他形式取得密碼、解密鑰或使用其他可允許未經授權接入的接入途徑。
16. 須在任何資訊系統運作前更改所有由供應商提供的預設密碼。
17. 如密碼可能已被洩漏或在接受保養及支援時披露予供應商，則須盡快更改密碼。
18. 須控制在登入時允許輸入不正確密碼的次數。如在登入時，輸入不正確密碼的次數超過預定限額，則應撤銷或鎖定該使用者身份。
19. 須有重設密碼的程序。該程序須包括核實申請者的身份，或將新密碼傳送至負責人或親自交付至申請者。

系統保安

20. 伺服器或電腦上應安裝反惡意軟件 / 防毒軟件，而該等軟件應每日自動更新惡意軟件 / 病毒的定義及掃描引擎 (scan engine)。
21. 不應爲提高系統性能而關閉反惡意軟件 / 防毒軟件。
22. 應每日及每週備份個人資料，而用作每週備份的媒體應移至獨立地方安全地儲存。
23. 如系統可連接互聯網，應考慮採用加密技術保護敏感的個人資料。
24. 如需在住所或海外 (如酒店) 遙距接入系統，則應使用虛擬網絡連線 (VPN) 等適當的網絡驗證及加密措施。
25. 僅公司提供的筆記本型電腦、通用串列匯流排 (USB) 及其他便攜式電腦設備可在公司網絡上使用。如須使用個人電腦設備，則須由管理層明確授權才可使用。而該等設備在每次接入公司網絡前，應經反惡意軟件 / 防毒軟件掃描及檢查。

實體設備保安

26. 放置主要伺服器及網絡基建設施的區域應以適當的安全措施加以保護，如許可的話，應配備氣體滅火系統、熱力或煙霧感應器及鎖上出入口。此外，應使用已上鎖的電腦設備機架加以保護。
27. 僱員應妥善保護分配予他們或由他們保管的電腦設備，如座枱式及便攜式電腦、可移動電腦設備或通用串列匯流排 (USB) 等儲存裝置。除非該設備已被鎖在安全地方，否則僱員不得任由電腦設備無人看管。

28. 資料中心、電腦室或相關區域須長期被鎖上，並備有出入記錄簿以供人員在每次出入時簽名記錄。外判承辦商於該地方工作時，應全程由獲授權人員陪同。

資料及資訊使用的規管及監控

概述

29. 應根據使用者的角色及職責以明確界定資料的查閱權限。
30. 高級管理層應明確界定資料查閱的權限及批核架構；應劃分職責，使某單一使用者不能同時擁有建立使用者身份及刪除使用者記錄的權限。
31. 應安裝螢幕保護程式密碼及定向螢幕過濾器，以防工作台顯示的敏感資料被未經授權讀取。
32. 應用系統的預設設定，應限制使用者從系統中複製敏感個人資料。如必需複製該等個人資料，應先取得高級管理層的明確批准。
33. 僱員不應從辦公室複製及帶走公務資料離開辦公室及 / 或將其下載至家庭或個人電腦設備上。如必需複製資料，則須事先取得高級管理層的批准。
34. 應防止儲存在家庭或個人電腦內的所有公務資料 (如有) 自動上載至互聯網 (如透過對等網絡軟件 (peer-to-peer software) 或檔案共享軟件)。
35. 如需在便攜式儲存設備上儲存個人資料，每次均須事先取得高級管理層的許可，並使用加密技術保護資料。
36. 爲保安理由，不成功的登入次數應以三次爲限，此後賬戶應被鎖定。如發現保安系統被試圖壞，須向系統管理人發出警報，並隨即採取補救措施。
37. 應妥善保護備份媒體。不應使用個人儲存設備備份公務資料。
38. 完整的備份副本須儲存在遠離系統的地方，並防止在運輸過程中遭到未經授權的接入、濫用或損壞。
39. 由互聯網下載的所有軟件和檔案須經防毒軟件掃描檢驗。
40. 載有敏感個人資料的電郵須加密才發送至外部網絡或電腦。
41. 僱員不應在工作時間內於公司工作台使用私人互聯網電郵服務，尤其是未經高級管理層事先批准而以該服務發送個人資料。
42. 不再使用的備份媒體須安全地棄置 (如透過焚化、壓碎或消磁)。

私隱

43. 如使用者長時間離開工作台 (如午餐、會議等)，則應登出載有敏感個人資料的應用程式 / 系統。
44. 應聘請外部獨立顧問每兩年進行一次私隱影響分析 (privacy impact analysis)，以復核及確保保護資料私隱的形式 / 方法是遵照業務需求及最新的監管要求。

記錄

45. 制定的記錄政策在技術許可的情況下須包括但不限於：
    - 使用者身份；
    - 登入、登出及其他重要事項 (如使用主管賬戶) 的日期及次數；
    - 獲分配的接入權限的任何更改；使用者賬戶及密碼的更改；
    - 系統配置、已安裝軟件及系統互連的任何更改；
    - 終端機名稱及位置；及
    - 嘗試接入系統成功及被拒的記錄。
46. 在技術許可下，須持續記錄以下於系統上的操作：
    - 嘗試未經授權的接入；
    - 擁有權限的使用者的操作；
    - 第三者供應商的接入；及
    - 接入系統的記錄檔案。
47. 特定的系統記錄須記下接入控制政策以外及有偏差的情況，以及其他安全相關的事件。
48. 應定期檢查記錄，尤其是處理 / 儲存的機密資訊系統 / 應用程式的記錄，同時兼顧日誌記錄的完備性與完整性。
49. 須嚴格限制記錄檔案的查閱權限，僅予擁有已核准的業務需要及適當查閱權的人。
50. 系統及應用程式的審計記錄應至少保存六個月。

第三者接入

51. 承辦商或次承辦商的所有僱員應遵守適用於地產代理僱員的相同資訊保安及資料私隱的規定。他們應知悉，若違反《政策》及相關保安指引及標準，可能導致違反規定並引致法律訴訟。
52. 須在合約上界定或制定適用於第三者的保安規定。該等規定須輔以供應商 / 承辦商 / 次承辦商的建議，但不得以任何形式降低或損害規定的保安水平。須針對所有供應商、承辦商及次承辦商撰寫及實行標準安全的條款，並對其加以施行，以應對各具體情況。
53. 除有高級管理層明確批准外，承辦商或次承辦商不得查閱個人資料。

僱員培訓及意識

54. 應每年向僱員提供有關個人資料私隱及保護的資訊講座或培訓課程。該等資訊講座或培訓課程可包括但不限於以下內容：
    - 最新資訊科技保安的威脅及其防範措施；

- 個人資料私隱法律及相關規定；及
- 個人資料私隱及保護的內部控制及規定。

55. 應在新僱員受僱三個月內，向其提供培訓。

56. 外判承辦商 / 次承辦商應同樣遵守適用於地產代理僱員的指引，並同樣受《政策》及其他相關文件規限。

- 完 -

附錄 C – 參考

標準及指引

政府資訊科技總監辦公室及其他政府部門發出的文件：

- 基準資訊科技保安政策 [S17]
  (http://www.ogcio.gov.hk/eng/prodev/download/s17_pub.pdf)
- 資訊科技保安指引 [G3]
  (http://www.ogcio.gov.hk/eng/prodev/download/g3_pub.pdf)

地產代理監管局發出的文件：

- 地產代理監管局公佈的操守守則
- 通告編號 09-10 (CR) – 資訊保安以妥善儲存資料

其他參考

- 《個人資料 (私隱) 條例》(第 486 章)