地 產 代 理 監 管 局
ESTATE AGENTS AUTHORITY

INFORMATION SECURITY AND PRIVACY PROTECTION POLICY AND GUIDELINES FOR ESTATE AGENTS

Table of Contents

1 PURPOSE

The protection of personal data privacy has become more and more important and complicated with the increasing use of information systems and digital devices. This document provides estate agents and their staff the minimum requirements for the protection of personal data privacy.

The policy statements within this document are developed for the reference of all estate agents and their staff at every level. Estate agents should note that the policy statements state clear regulatory requirements with which estate agents and their business partners should comply. They are written at such a level that allows estate agents to apply specific control and protection where appropriate.

For specific recommendations on standards and guidance on technical requirements on information systems, please refer to a separate set of guidelines for small agencies[1] and another set for medium and large agencies in the appendices to this document.

This document is not meant to be a comprehensive model policy nor shall it prejudice the exercise of the regulatory functions and powers of the Estate Agents Authority under the Estate Agents Ordinance.

[1] For the purpose of this document, small agencies are those with 4 offices or less and medium and large agencies are those with 5 or more offices.

2 DEFINITIONS AND CONVENTIONS

2.1 Definitions

1. Availability	Information systems should be available to users at any given or specified period of time.
2. Computer Room	A dedicated room for hosting computer equipment.
3. Confidentiality	Only authorised persons are allowed to know or have access to the information stored in or processed by Information Systems in any aspects.
4. Contractors / Sub Contractor	Persons employed by a company which provides services directly or through another company irrespective of the employment period and terms.
5. Data Subject	In relation to personal data, the individual who is the subject of the data.
6. Data User	In relation to personal data, a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of data.
7. Guidelines	Recommended effective security practices that should be implemented wherever possible.
8. Information	Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automatic means. Information is relayed in a variety of methods, such as spoken communication, written documentation or computer networks. Information is stored and retrieved in several formats which include but are not limited to: computer databases or transmissions, tapes, diskettes, computer generated reports, written documentation, e-mail messages, voice mails, meeting minutes and working papers.
9. Information Security	The protection of information assets from sender to receiver, or from client to server. Information protection usually means protecting the “Confidentiality”, “Integrity” and “Availability” of data. Security should be considered an enabler of business, but not an inhibitor.

10. Information System	An electronic information system that processes data electronically through the use of information technology, which includes but is not limited to: computer systems, servers, workstations, terminals, storage media, communication devices and network resources.
11. Information User	The person who officially needs to view, read or use (either on-line or off-line) the data or information from an information system.
12. Integrity	Only authorised persons are allowed to make changes to the information stored in or processed by information systems in any aspects.
13. Staff	Persons employed irrespective of employment periods and terms. Wherever applicable in context, this term also covers staff of service contractors.
14. Standards	Mandated actions that specify the proper use of the computer resources, and act as a control for the security policy.
15. System Administrator	A person responsible for the day-to-day operation of the system and network resources.
16. System User	A person who is responsible for inputting to or retrieving from an information system the data or information as and when required in the course of discharging his/her duties.

2.2 Conventions

The following is a list of conventions used in this Policy:

Shall	the use of the word ‘shall’ indicates a mandatory requirement.
Should	the use of the word ‘should’ indicates a requirement for good practice, which should be implemented whenever possible.
May	the use of the word ‘may’ indicates a desirable requirement.

3 CONTROLLING AND REGULATING THE RIGHT TO ACCESS DATA: NEED TO KNOW

3.1 Management

3.1.1 The protection of clients' personal data is the responsibility of every staff member. Senior management or their delegates shall educate their staff about this Policy and strengthen their awareness on personal data privacy protection.

3.1.2 Least privilege principle shall be enforced when resources and privileges of information systems are assigned to users.

3.1.3 Personal data of clients should not be exposed to external workers or contractors. Should exposure become necessary, precautionary measures shall be implemented.

3.1.4 Estate agents shall ensure the confidentiality, integrity and availability of information and all other security aspects of information systems under their control including outsourced systems.

3.1.5 The roles and responsibilities in data privacy and protection of each specific level of staff should be clearly defined.

3.1.6 Information security audit on data protection should be done regularly.

4 SYSTEM INTEGRITY

4.1 User Identification

4.1.1 Each user of the information system shall have his own user ID in accessing the system and his system privilege should be reviewed regularly.

4.1.2 Users are responsible for all activities performed with their user IDs.

4.1.3 A strict password policy that details at least the minimum password length, initial assignment, restricted words and format, password life cycle, and includes guidelines on suitable system and user password selection should be defined.

4.2 System Security

4.2.1 Anti-malware software shall be installed on servers or computers where sensitive personal data are stored.

4.2.2 Regular backup should be done on personal data to ensure protection against accidental erasure or sabotage.

4.3 Physical Equipment Security

4.3.1 All information systems shall be placed in a secure environment or attended by staff to prevent unauthorised access.

4.3.2 Staff should pay attention in protecting the computer equipment provided to them by the company with high degree of protective measures.

4.3.3 Data centres, computer rooms or areas where critical systems or computers are kept shall be properly protected and their access should be strictly controlled.

5 REGULATING AND MONITORING THE USE OF DATA AND INFORMATION

5.1 General

5.1.1 Data access rights shall be clearly defined and reviewed by management regularly, and such privileges should be granted on a need-to-know basis.

5.1.2 A formal authorization process should be put in place. All access to sensitive personal data shall be documented as a control of access rights allocation.

5.1.3 Precautionary measures should be enabled to protect sensitive information from unauthorized access when a user is away from his/her workstation.

5.1.4 Staff should not copy official data away from their offices and/or load them onto their home or personal computing devices. Should such action become necessary, prior approval from senior management shall be obtained.

5.1.5 Management should ensure that third party service providers observe and comply with this Policy and other information security requirements issued by the relevant authorities.

5.1.6 Access to the company network should be protected with justified security measures such as firewall, anti-malware/virus software, and/or intrusion detection mechanism.

5.1.7 Connecting privately owned computer devices, including personal notebook computers, PDAs, USB storage devices, etc., to company network shall be strictly prohibited unless approved by senior management.

5.2 Privacy

5.2.1 Management should reserve the right to examine all information stored in or transmitted by its information systems to ensure compliance with the Personal Data (Privacy) Ordinance.

5.2.2 All applicable requirements on the use of sensitive data should be complied with. Personal data collected and maintained shall:

- be used only for the stated purpose for which they were collected;
- be kept for the amount of time required by law or regulations or for as long as they are required but not longer than is necessary;
- be erased according to the requirements of the law and as recommended by the relevant guidelines on data disposal; and
- not be disclosed without specific consent from the data subjects.

5.3 Logging

5.3.1 Senior management shall ensure that adequate logging of activities of the information systems / applications under their purview is defined.

5.3.2 Logs shall be retained for a period commensurate with their usefulness as an audit tool. During this period, such logs shall be secured and can only be read by authorised persons.

5.3.3 Logs shall not be used to profile the activity of a particular user unless it relates to a necessary audit activity supported by senior management. The logs produced in particular system shall only be used to check compliance with the access control policy and the controls implemented. They shall not be used as a means to profile user activities, unless this relates to particular audit or incident investigation activity.

6 STAFF TRAINING AND AWARENESS

6.1.1 Regular information sessions or training on personal data privacy and protection and latest information security trends should be provided to staff whenever possible.

6.1.2 Regular internal memos and circulars on the privacy and protection of personal data shall be provided to staff to ensure that they are aware of the prevailing information threats and how they could comply with this Policy in the course of their work.

- END -

APPENDIX A – GUIDELINES FOR SMALL AGENCIES

PURPOSE

This set of guidelines aims to provide estate agents with 4 offices or less with more specific advice on "HOW" the Information Security and Privacy Protection Policy for Estate Agents (the "Policy") could be complied with.

The guidelines stated here are not mandatory requirements but they should be referenced as a model for technical standard for compliance. Estate agents should note that the guidelines are suggestions only and they should define their own organizational requirements on data privacy and protection. Estate agents should also implement security measures appropriate for their level of risk exposure and available resources. However, the technical protection implemented by estate agents should be not be lower than the level set out in the Policy.

MANAGEMENT CONTROL ON DATA ACCESS

1. Necessary resources to support initiatives on data privacy protection and information security should be provided.
2. Rights of system administrator to access applications containing personal data should be separate from those given to general users; IT staff or contractors who are responsible for maintaining computer systems shall be restricted from accessing sensitive personal data.
3. Estate agents shall ensure the overall security of the application system and its data to prevent information leakage or unauthorized disclosure.
4. Internal memo in alerting staff on the following topics should be issued regularly:
   - latest IT security threats and counter-measures;
   - personal data privacy laws and related requirements; and
   - internal control and requirement on personal data privacy and protection.
5. External resources should be hired to assess the security of IT systems periodically.

SYSTEM SECURITY AND PROTECTION

6. Each user shall have only one user ID for each application; shared password should not be encouraged.
7. When a staff member is removed from his/her job due to dismissal, resignation, or change of position permanently, his/her user ID should be suspended or locked promptly.
8. User passwords should be at least 6 characters long with the combination of alpha-numeric characters; a password should be changed every six months.
9. Passwords shall be memorized and not written down anywhere in the office.

10. When new computing equipment is installed, the vendor-supplied / default passwords shall be changed before any information system is put into operation.
11. Anti-malware/virus software should be installed on servers or computers with daily and automatic update of malware/virus definition and scan engine.
12. Anti-malware/virus software should not be turned off in order to enhance system performance.
13. Full backup on personal data should be done regularly.
14. If remote access from home or overseas such as hotels, etc. is required, proper network security technology such as VPN or SSL should be used.
15. The location used to host computer equipment should be locked when the office is unattended.
16. Staff should properly safeguard computing equipment such as desktop and portable computers, mobile computing devices or USB storage devices assigned to them or in their possession; staff shall not leave computing equipment unattended unless it is properly protected in a locked environment.
17. External contractors should carry out their work in the presence of the estate agent's staff; computing equipment should not be allowed to be taken away for service.

REGULATING AND MONITORING THE USE OF DATA AND INFORMATION

General

18. Data access privileges should be carefully determined before they are assigned to staff.
19. Screen saver password and directional screen filter should be installed to prevent unauthorized access to sensitive data displayed.
20. Backup media should be properly protected under locked environment; personal storage devices should not be used to backup official data.
21. All software and files downloaded from the Internet shall be screened and verified with anti-virus software.
22. Sensitive personal data shall not be sent via Internet e-mail.
23. Staff should not use private Internet e-mail service during office hours on company workstations, especially using it for transmitting personal data, without the prior approval of senior management.
24. Backup media and computers that are no longer used shall be disposed of securely (e.g. by incinerating, shredding, or magnetic degaussing).
25. Users should logout from the application / system with access to sensitive personal data when they are away from their workstations for an extended period (i.e. lunch, meetings etc.).
26. The effectiveness of data privacy and protection mechanism should be reviewed regularly.

27. System usage history should be recorded for future security review when necessary. Some of the suggested items to be recorded are:
    - user IDs;
    - dates and times of log-in and log-off and other key events (e.g. use of supervisor accounts);
    - any changes of access rights allocated; changes in user accounts and passwords;
    - any changes of system configuration, software installed and system interconnections; and
    - records of successful and rejected system access attempts.
28. Access to log files shall be strictly limited, and system and application audit logs should be retained for a period of at least six months.

Third-Party Access

29. All staff of contractors or subcontractors should comply with the same information security and data privacy requirements applicable to the staff of the estate agents. They should know that violation of this Policy and related security guidelines and standards could result in compliance violation and legal action.
30. Security requirements applicable to third parties shall be defined or formalized on a contractual basis. The requirements shall be complemented with supplier / contractor / subcontractor proposals but should in no way downgrade or compromise the required security level. Standard security clauses shall be written and imposed on all suppliers, contractors and subcontractors to meet precise situations.
31. Contractors or subcontractors shall not be allowed to access personal data unless explicitly approved by the estate agent.

- END -

APPENDIX B – GUIDELINES FOR MEDIUM AND LARGE AGENCIES

PURPOSE

This document aims to provide estate agents with 5 or more offices with technical advice on "HOW" the Information Security and Privacy Protection Policy for Estate Agents (the "Policy") should be complied with.

The guidelines stated in this document are not mandatory requirements but they should be referenced as a model for technical standard for compliance. Estate agents should note that the guidelines are suggestions only and they should define their own organizational requirements on data privacy and protection. Estate agents should also implement security measures at the level appropriate to their level of risk exposure and available resources. However, the technical protection implemented by estate agents should not be lower than the level set out in the Policy.

CONTROLLING AND REGULATING THE RIGHT TO ACCESS: NEED TO KNOW

Management

1. Management should provide necessary resources to support initiatives on educating and training employees on data privacy protection and information security.
2. Proper segregation of duties for users and administrative staff of the IT systems containing sensitive personal data shall be clearly defined and implemented in order to avoid conflict of interests.
3. Privileges assigned to each user, both internal or external employees, should be approved by management on a need-to-know basis. Such privileges should also be reviewed periodically for consistency and operational purposes.
4. Sufficient segregation of duties shall be applied to avoid conflict of interests in administering information system by IT staff or contractor.
5. Management shall ensure the confidentiality, integrity and availability of information and all other security aspects of information systems under its control including outsourced systems.
6. External workers or contractors should be required to sign a non-disclosure agreement when clients' personal data could be exposed during the course of their services.
7. IT security risk assessment and audit on IT systems and infrastructure should be performed every two years or so by internal or external auditor to ensure integrity and confidentiality.

SYSTEM INTEGRITY

User Identification

8. Each user ID shall uniquely identify only one user. Shared or group user IDs should be discouraged unless explicitly approved by management and formal endorsement procedure should be implemented and recorded.
9. Strict application procedure should be enforced on shared password creation and usage. Shared user ID and password should be used only under critical circumstances and the password shall be changed after each use.
10. System privileges of users should be reviewed every six months or when the job functions of a staff member has been changed.
11. When a staff member is removed from his/her post due to dismissal, resignation, or change of position permanently, his/her user ID should be suspended or locked promptly.
12. User passwords should be at least 6 characters long with the combination of alpha-numeric characters, and the password should be changed every six months. If the application system has the capability of issuing automatic reminders for password change, this option should be turned on.
13. Passwords shall not be shared or divulged unless necessary (e.g., helpdesk assistance, shared PC and shared files). If passwords must be shared, explicit approval from senior management must be obtained.
14. Passwords shall always be well protected when held in storage or when transmitted over networks wherever possible. Compensating controls shall be applied to reduce the risk exposure of information systems to an acceptable level if encryption is not feasible.
15. Staff is prohibited from capturing or otherwise obtaining passwords, decryption keys, or any other access control mechanism, which could permit unauthorised access.
16. All vendor-supplied default passwords shall be changed before any information system is put into operation.
17. All passwords shall be promptly changed if they are suspected of or being compromised, or disclosed to vendors for maintenance and support.
18. Controls shall be put in place to limit the number of log-in attempts with invalid passwords. This shall be accomplished by either revoking or locking the user ID upon a pre-defined number of consecutive invalid attempts.
19. A process shall be put in place to reset passwords. The process shall either include the checking of the identity of the requestor or otherwise the new password shall be sent to a responsible manager or delivered in person to the requestor.

System Security

20. Anti-malware/virus software should be installed on servers or computers with daily and automatic update of malware/virus definition and scan engine.
21. Anti-malware/virus software should not be turned off in order to enhance system performance.

22. Full backup on personal data should be done with daily and weekly basis, and the weekly backup media should be moved to separate locations for secure storage.
23. Encryption technology should be considered to protect sensitive personal data if a system containing such data is reachable from the Internet.
24. If remote access from home or overseas such as hotels is required, proper network authentication and encryption such as VPN should be used.
25. Only officially provided notebook computers, USB devices, and other portable computing devices should be used on company network. If personally owned computing devices must be used, explicit authorization shall be given by management. Such devices should be scanned and checked with anti-malware/virus software before they are connected to the company network every time.

Physical Equipment Security

26. The location used to host critical servers and network infrastructure should be protected with proper security measures such as gas based fire suppression system if possible, heat or smoke sensors and locked door(s) for access. In addition, equipment should be protected in a locked computer equipment rack.
27. Staff should properly safeguard the computing equipment such as desktop and portable computers, mobile computing devices, or USB storage devices assigned to them or in their possession, and shall not leave the equipment unattended unless it is properly protected in a locked environment.
28. Data centres, computer rooms or areas shall be locked at all times with access log-book for signing in and out every time a person enters the premises. External contractors should be escorted by authorized personnel at all time.

REGULATING AND MONITORING THE USE OF DATA AND INFORMATION

General

29. Data access privileges should be clearly defined based on the users' roles and responsibilities.
30. Senior management should define clearly the data access authorization and approval framework; segregation of duties should be applied so that no single user can create user IDs and erase user records.
31. Screen saver password and directional screen filter should be installed to prevent unauthorized access to sensitive data displayed on the workstations.
32. Application systems should, by default, control users from copying sensitive personal data from the systems. If such capability is required, senior management should provide explicit approval.
33. Staff should not copy official data away from their offices and/or load them onto their home or personal computing devices. If such action is necessary, prior approval of senior management shall be obtained.

34. All official data stored in the home or personally owned computer, if any, should be protected against automatic uploading of data to the Internet (e.g. through peer-to-peer software or file sharing software).

35. If storing of personal data on a portable storage device is required, prior permission from senior management shall be sought on each occasion and encryption technology should be used to protect the data.

36. Unsuccessful login attempts should be limited to 3 times only after which the account should be locked for security purposes. Alert shall be sent to system administrator for checking security breach attempt and remedial action should follow.

37. Backup media should be properly protected. Personal storage devices should not be used to backup official data.

38. Integrity copies of backups shall be stored at a remote distance from the system and be protected against unauthorized access, misuse, or corruption during transportation.

39. All software and files downloaded from the Internet shall be screened and verified with anti-virus software.

40. E-mail containing sensitive personal data shall be encrypted during transmission to external network or computer.

41. Staff should not use private Internet e-mail service during office hours on company workstations, especially using it for transmitting personal data, without the prior approval of senior management.

42. Backup media that are no longer used shall be disposed of securely (e.g. by incinerating, shredding, or magnetic degaussing).

Privacy

43. Users should logout from their application / system which has access to sensitive personal data when away from workstations for an extended period (i.e. lunch, meetings etc.).

44. External, independent consultants should be hired to perform privacy impact analysis every two years to review and ensure data privacy protection is according to business needs and up to date with the latest regulatory requirements.

Logging

45. The defined logging policies shall include but not be limited to the following wherever technically feasible:

    - user IDs;
    - dates and times of log-in and log-off and other key events (e.g. use of supervisor accounts);
    - any changes of access rights allocated; changes in user accounts and passwords;
    - any changes of system configuration, software installed and system interconnections;
    - terminal identity and location; and

- records of successful and rejected system access attempts.

46. The following system-based activities shall be logged continually whenever technically feasible:
    - unauthorized access attempts;
    - privileged user activity;
    - access by third party vendors; and
    - access to system log files.
47. Logs produced in a particular system shall record exceptions to or deviations from the access control policy, and other security relevant events.
48. Regular checking of log records, especially on system / application where classified information is processed / stored, should be performed, not only on the completeness but also the integrity of the log records.
49. Access to log files shall be strictly limited to those individuals with an approved business needs and appropriate access rights.
50. System and application audit logs should be retained for a period of at least six months.

Third-Party Access

51. All staff of contractors or subcontractors should comply with the same information security and data privacy requirements applicable to the staff of the estate agents. They should understand that violation of this Policy and related security guidelines and standards could result in compliance violation and legal action.
52. Security requirements imposed on third parties shall be defined or formalized on a contractual basis. The relevant clauses shall be complemented with supplier / contractor / subcontractor proposals but in no way downgrade or compromise the required security level. Standard security clauses shall be written and imposed on all suppliers, contractors and subcontractors to meet precise situations.
53. Contractors or subcontractors shall not be allowed to access personal data unless explicit approval is given by senior management.

STAFF TRAINING AND AWARENESS

54. Information sessions or training on personal data privacy and protection should be provide to staff annually. Such information sessions or training could include but not limited to the following:
    - latest IT security threats and countermeasures;
    - personal data privacy laws and related requirements; and
    - internal control and requirement on personal data privacy and protection.
55. New staff should be provided with training within 3 months of employment.

56. External contractors / subcontractors should follow the same guidelines and be subject to the same requirement set out in the Policy and other related documents applicable to the staff of the estate agents.

- END -

APPENDIX C – REFERENCES

Standards and Guidelines

Documents issued by the Office of the Government Chief Information Officer and other government agencies:

- Baseline IT Security Policy [S17]
  (http://www.ogcio.gov.hk/eng/prodev/download/s17_pub.pdf)
- IT Security Guidelines [G3]
  (http://www.ogcio.gov.hk/eng/prodev/download/g3_pub.pdf)

Documents issued by EAA:

- Code of Ethics promulgated by the Estate Agents Authority
- Circular No. 09-10 (CR) - Information Security for Privacy Protection

Other References

- Personal Data (Privacy) Ordinance (Cap. 486)