

Railway Housing Association

**INFORMATION
SECURITY
POLICY
(Computer Held Information)**

INFORMATION SECURITY POLICY - SUMMARY

DO

- DO Understand that Information Systems Security and Confidentiality is EVERYONE's responsibility.
- DO Ensure you read and understand the Information Security policy and the *policies on the use of E-mail and the Internet*.
- DO Report immediately any threat to, or breach of information system security to your Line Manager and the Information Security Officer.
- DO Contact the Information Security Officer for further guidance or advice on information systems security.
- DO Ensure that the equipment on your desk or work area and which you use as part of your job is kept as secure as possible.
- DO Ensure that you are familiar and confident with the systems you are using.
- DO Ensure that all visitors are supervised and do not gain access to restricted areas (e.g. Computer Rooms) without prior approval from the Information Security Officer or designated authority.
- DO Keep your password(s) secure and change them regularly in accordance with the Information Security Policy
- DO 'Lock' or Log out of your Computer when leaving your desk or work area.
- DO Switch off your Computer when you leave your desk for longer periods of time.
- DO Dispose of printouts containing personally identifiable data securely by shredding.
- DO Report any emails containing obscene material to your Line Manager and the Information Security Officer.

DON'T

- DON'T Assume that the responsibility for Information Systems Security rests with someone else.
- DON'T Position or leave computer equipment where it may be easily damaged or stolen.
- DON'T Leave visitors unattended in areas where computer equipment is kept or used.
- DON'T Allow visitors to enter secure areas (e.g. Computer Rooms) without the prior approval of the Information Security Officer or designated authority.
- DON'T Move any computer equipment without notifying the Information Security Officer.
- DON'T Take computer equipment off-site without obtaining authorisation.
- DON'T Leave computer equipment taken off-site unattended in public places, in your car or any other location where theft or damage may occur.
- DON'T Dispose of computer equipment without consulting The Information Security Officer.
- DON'T Ignore potential or actual breaches of security or confidentiality.
- DON'T Install software or load disks containing software or data from external sources, or that have been used in external equipment, without obtaining authorisation from the Information Security Officer.
- DON'T Reveal your password to anyone else.
- DON'T Let other users use a computer using your login details.
- DON'T Leave your computer logged in when you leave your desk or work area.

1. Introduction

1.1 The Need for an Information Security Policy

This document describes Railway Housing Association policy on information security and employees responsibilities for security of information held on the Association's IT Systems. *It should be read in conjunction with the Association's Data Protection, Confidentiality and Document Retention policy.*

Railway Housing Association holds and manages a great deal of personal and confidential data relating to applicants, tenants, contractors, suppliers and employees. Increasing reliance is placed on computers to store and manipulate this information and with the ever-easier ways by which information can be passed around both internally and externally via other connected networks, it is important that a consistent approach is adopted to safeguard this information.

This policy is intended to broadly comply with the framework of BS ISO / IEC 17799.

The Information Security Policy addresses the following issues;

- **Confidentiality:** Ensure that information is accessible only to those authorised to have access.
- **Integrity:** Safeguard the accuracy and completeness of information and processing to ensure confidence in the authenticity of the information.
- **Availability:** Ensure that authorised users have access to information when required.

2. Information Security Policy Statement

2.1 The Policy aims to ensure that:

- All of the Association's computer systems are secure and confidential. In particular that these are operated in accordance with BS ISO / IEC 17799 and relevant Association policies such as those in accordance with the Data Protection Act 1998.
- All staff are aware of this policy, the need to ensure appropriate, secure and confidential handling of all personal and business sensitive information and their responsibilities in maintaining information security.
- Confidentiality, integrity and availability are maintained.
- Procedures to detect and resolve security breaches are in place.

Failure by any employee to comply with the policy and its guidelines will be viewed as a serious matter and may result in disciplinary action.

Where employees believe that it is not possible to meet the policy, this must be brought to the attention of their Functional Manager and action agreed and notified to the appropriate management level within the Association.

2.2 Scope

This policy applies to:

- All Association employees whilst engaged in work for the Association at any location, on any computer.
- Any other uses by Association employees which identifies the individual as Association employee or which could bring the Association into disrepute on any computer or network connection.
- Other persons working for the Association including agency staff, persons engaged on Association business or persons using Association equipment and networks.
- Any individual or company granted access to the Association network.

2.3 Review and Maintenance

This policy will be subject to regular review to ensure accuracy and relevancy. If revised, all staff will be alerted to the new version.

3. Association Responsibilities

3.1 Introduction

Security is all employees' responsibility to ensure information is, as appropriate, confidential, accurate and available to authorised users.

This section describes the different areas of responsibilities for ensuring that the Association's information remains secure. There is a clear division of responsibilities between the Board of Trustees, Senior Management Team, the appointed Information Security Officer, Level D Line Managers and Employees.

3.2 Board of Trustees

The Board of Trustees has overall responsibility for all matters relating to information security.

3.3 Senior Management Team

The Senior Management Team should:

- ensure that all current, new and temporary staff are instructed in their security responsibilities.
- determine which individuals are to be given authority to access specific information. Levels of access to specific systems should be on a job function need.
- ensure that the Information Security Officer is notified of new employees to allow access rights to be appropriately established from effective dates.

3.4 Information Security Officer

The Finance Manager will have specific responsibilities as Information Security Officer for the implementation and enforcement of the Information Security Policy and has security management responsibilities for:

- monitoring and reporting on the state of Information Management & Technology security within the Association.
- ensuring that the Information Security Policy is implemented throughout the Association, developing and enforcing procedures to maintain security.
- ensuring compliance with relevant legislation.
- ensuring no unauthorised staff are allowed to access any of the Association's computer systems or information, as such access could compromise information integrity.

- ensuring that the Association's employees are aware of their ongoing responsibilities and accountability for information security.
- monitoring for actual or potential information security breaches.
- ensuring the Application Service Provider (ASP) maintains security in line with the information security policy.
- reporting security issues to the Chief Executive and / or Functional Manager.
- providing advice on information security.

3.5 Level D Managers

The Level D Managers should:

- understand the risk to the computer assets and the information that is held on them.
- conform to the Information Security Policy.
- Through normal staff supervision, report any security incidents to the Information Security Officer. These include the sharing of confidential information such as passwords, excessive personal or inappropriate use of email and unauthorised personal use of any of the Association's ICT facilities.
- ensure that all their staff using computer systems are trained in their use.
- implement procedures to minimise the Association's exposure to risk through fraud, theft, or disruption of its systems; such as segregation of duties.
- ensure that procedures are in place so that Functional Managers advise the Director of Finance or Finance Manager immediately about staff changes affecting computer access (for example job function changes / leaving department or Association) so that passwords may be withdrawn / deleted.
- ensure their staff are working in a manner consistent with the Information Security Policy.
- inform the Information Security Officer of any security issue that members of staff raise in connection with their work.

3.6 All employees

Employees, including those under contract and agency staff, are:

- responsible for conforming to the Information Security Policy.
- required to bring to their Manager or Information Security Manager's attention areas of concern regarding information security.
- required to abide by the terms of the Data Protection Act (1998).
- ensure they have familiarity with the Association's software systems where applicable i.e. Context, Sun, Windows.

All staff are responsible for ensuring that no actual or potential security breaches occur as a result of their actions. The Association will investigate all suspected / actual security breaches and report to the appropriate bodies.

Security breaches may result in disciplinary action

3.7 Application Service Provider (ASP – Civica Connect)

Civica Connect must ensure (in accordance with the Service Level Agreement) that the physical security of servers, event log monitoring and logical access controls is maintained.

- Only authorised staff are given access to the Association's servers, files and information.
- Access logs are kept up-to-date and available to the Information Security Officer at all times.
- Information will be held within a data-certified fireproof safe, as required, to facilitate a maximum loss of one calendar week of information destroyed as a result of local building or system damage.
- All back-ups will be maintained securely and will be erased when no longer required.
- All actual or possible breaches of security are reported to the Information Security Officer.

4. Risk

Any security measures must be viewed as necessary in order to protect the Association against a risk of an event occurring or to reduce the impact of such an event. Some of these events may be deliberate acts of damage and others may be accidental.

The risk assessment of IT will form part of the Association's overall Risk Register and will be reviewed periodically. These will account for changes in business requirements and priorities; consider new threats and vulnerabilities and confirm that current controls are effective and appropriate.

All staff should consider the risks associated with the computers and the information that is held on them. All staff are responsible for reporting any apparent shortcomings of security measures to their Functional Manager.

5 Computer Records Policy

This section describes the policy and principles for using all computer systems and the storing and handling of information.

5.1 Computer Information Systems

5.1.1 Physical Security

- All access to computers located within Association property must be restricted through the use of the same precautions that are taken for other valuable assets of the Association. Such restrictions include ensuring doors are closed / locked properly, the use of door entry codes and only authorised staff are given access to controlled areas.
- Visitors should be met at reception and accompanied wherever possible.
- Computers that are particularly valuable or that hold critical information, such as servers, will be located in secure rooms that have lockable doors.
- Staff must surrender door keys to secure areas on termination of employment.
- All computer assets will be sequentially tagged and each machine will have its serial number recorded.
- Computers must not be moved without notifying the Director of Finance or Finance Manager in advance.
- Employees should make every effort to ensure that fire, flood and accidents do not cause damage.

- Equipment must be sited to minimise the risk of accidental damage. Common hazards include drinks, cups, food and overstraining of leads when a machine is moved.
- Excessive paper should not be stored on or near computer equipment due to the risk of fire; computers generate a lot of heat in use and need adequate ventilation.
- Any suspected damage, which may not be visible externally (for example after dropping a computer), must be reported to the Director of Finance or Finance Manager for checking before continued use.

5.1.2. Equipment Maintenance

- All critical processing equipment, including file servers, will be covered by appropriate maintenance agreements.

5.1.3 Information Storage

- No information must be held that breaches the Data Protection Act (1998).
- All staff must comply with Data Protection legislation and must not be allowed to access information until line managers are satisfied that they understand and agree these responsibilities.
- ***Information that is no longer required should be disposed of or archived securely in accordance with the Association's Data Protection, Confidentiality and Document Retention Policy.***
- ***Information should be stored within the shared directory. If you store any information (files and folders) in any place other than the Shared Directory eg U:\ drive, you MUST disclose the contents of these files and folders in writing to the Data Protection Officer.***
- Paper records containing personal information must be disposed of securely. Anything containing personal and/or confidential information that does not require archiving must be shredded after use.

5.1.4 Information Back-up

Information must be stored on the systems servers via the shared directory in order to maintain confidentiality, availability and integrity of that information and reduce impact of breaches in physical security.

Data located upon network servers will be backed up in accordance with the Service Level Definitions as stated in appendix B of the ASP Service Level Agreement.

Such information will be held within a data-certified fireproof safe, as required, to facilitate a maximum loss of one calendar week of information destroyed as a result of local building or system damage.

All back-ups will be maintained securely and will be erased when no longer required.

5.1.5 Disposal of Equipment

- All data storage devices will be removed of sensitive data before disposal through being physically destroyed or securely overwritten. If any disposal or physical destruction is carried out by a third party, a certification from that third party will be sought.
- ***Obsolete computer equipment may have little or no residual financial value - but may still hold valuable information and/ or software. Pending removal of data, care should be taken to ensure secure storage of equipment and control of access.***

5.1.6 Business Continuity

All designated systems will be covered by the Association's disaster recovery plan. This is required to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

5.2 Networks

5.2.1 Local and Wide Area Networks

Through connection to the Association's network it is possible to receive and forward information to other users of the network and other organisations networks using, for example, electronic mail.

If information is copied between the Association's systems and that of another network, then employees should ensure that any confidential information remains secure and that the recipient system has the same or greater standard of security protection.

Should employees receive, identify how to, or gain access to unauthorised information on any networks then this event must be reported to their Functional Manager.

5.2.2 User Access to Network, Computers and Applications

Only Association staff or authorised support agents are authorised to access Association computers and the information held on them. Unauthorised access may contravene the Computer Misuse Act (1990) and Data Protection Act (1998) and other legislation leaving **the user** open to prosecution.

No individual will be given access to a live system unless properly trained and made aware of their security responsibilities.

Access to the network will be protected by unique user names and passwords. Employees must be granted access only to those areas that they require to perform their duties.

5.2.3 E-Mail and Internet Use

The office systems at the Association are a valuable asset that enables employees to benefit from efficient office communication. Authorised users should ensure care is taken when using electronic mail and the Internet as failure to do so can reflect poorly on the individual and / or the Association.

Also, the forwarding of e-mail to external destinations is an important business need. However, care must be exercised where there is a risk of forwarded e-mail being accessed by unauthorised individuals. This includes forwarding to home computers.

E-mail is identical to any other form of the Association's business correspondence and can be legally binding or challenged. **All staff must comply with the Association's E-Mail policy.**

Staff with access to the Internet shall use it for appropriate business purposes and should comply with the Association's Internet Acceptable Use Policy.

5.2.4 Notification of Staff Changes

Functional Managers will be responsible for the notification of new employees to the Director of Finance or Finance Manager. Written communication e.g. an email, should be sent to the Director of Finance or Finance Manager specifying what access rights are to be established to which applications stating the effective dates.

The Chief Executive's PA will advise the Director of Finance or Finance Manager about staff changes affecting computer access for those staff leaving the Association. Level D Managers should inform the Director of Finance or Finance Manager of change in employees job function so that access rights may be amended or deleted, from effective dates. This should be done by the way of written communication.

5.3 Desktop Policy

5.3.1 Use and Installation of Software

Under no circumstances should software, other than that approved and authorised, be loaded onto Association's computers. Employees must not use disks previously used from external sources or download software without first getting permission from the Director of Finance or Finance

Manager. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to prosecution.

5.3.2 Computer viruses

Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses. This can cause serious disruption to both the user and the Association's systems.

The Association's IT systems run up-to-date anti-virus software in accordance with the ASP agreement, however employees should not run or use software on stand-alone applications that has not been checked for viruses.

Staff must contact the Director of Finance or Finance Manager if a virus incident is suspected.

5.3.3 Password Guidance

Passwords have a valuable role in protecting systems from unauthorised access and must:

- not be names or have other connections to the user.
- be changed regularly and not be related to previous passwords.
- be kept secret and not written down.
- not be shared.

Furthermore:

- **Citrix/Windows 2000** login are subject to 90 day password change. Passwords are required to be six characters minimum.
- **CTX (application)** are subject to 90 day password change. Passwords are required to be six characters minimum alphanumeric. Password must contain at least one numeric.
- **SUN Accounts (application)** are subject to 90 day password change. Passwords are required to be five characters minimum.
- Three bad login attempts will result in the user being locked-out. The Director of Finance or Finance Manager should be notified if this occurs.

- A default password will be used for all new users set-up by the ASP. The user will then be prompted to change the password upon first login.
- A default password is used for users that require a new password not in the normal 90 day change cycle. This will normally be as a result of the user 'locking' their citrix session or if the user has forgotten their password. Password changes will be actioned by the ASP upon request from the Director of Finance or Finance Manager. The user will then be prompted to change the password upon first login.
- Only the individual to whom it is issued should use that password.
- Users must Log off or user-lock their computer via the password protected screen-saver (see 5.3.4 below), if a computer is left unattended.
- Users must not attempt to gain access to systems or facilities for which they have not been duly authorised, or by trying to use or guess another staff member's User-ID and password.
- Only in exceptional circumstances and not without agreement of a Functional Manager will the ASP be requested to change a user's password to grant temporary access to an account. After-which, a new password will be generated before further access to system.

This policy will ensure proper auditing of accesses made can be maintained and security of original user account is not compromised.

5.3.4 Clear Screen Policy

Workstations will require a username and password to be entered before accessing any of the Association's systems on that machine. A screen saver with password protection will be used on all Thin tune computers with an inactivity time out set to fifteen minutes. The user will then be required to enter their *Citrix* password to gain access to their desktop.

6 Access to the Association's IT systems by Application Service Provider.

6.1 Introduction

This outlines the steps to be taken in reference to access to the Association's network and computer systems by the Application Service Provider, typically providing IT systems management and support.

6.2 Access

All access by the ASP is to be managed under a clear protocol agreed in accordance with the ASP agreement.

Any on-site support is to be provided by nominated, identifiable individuals from the ASP's company with their work closely monitored with activities logged.

6.3 Procedures

Each support call will be logged by the Finance Manager or nominated member of staff in their absence.

Any access by the ASP to the Association's systems will be identified through:

- Citrix Administrator Logon Log
- Unix 'root' Logon Log

Where possible, access to the Association's Servers will be matched to the support call log.