ICT SECURITY POLICY

Owner	Andrew Martin
Sponsor	Andrew Martin

Version Control	**Date of Current Review**	**Date of Next Review**	**Reviewed by**
V1	March 2021	March 2024	Board

CORPORATE FIT	
Internal Management Plan	✓
Risk Register	✓
Business Plan	✓
Regulatory Standards	✓
Equalities Strategy	
Legislation	✓

1. Introduction

1.1. The purpose of the Policy is to protect Albyn Housing Society Group's ("Albyn") information assets from all threats, whether internal or external, deliberate or accidental.

1.2 It is the policy of Albyn to ensure that:

- information will be protected against unauthorised access.
- confidentiality of information will be assured.
- integrity of information will be maintained.
- regulatory and legislative requirements will be met.
- business continuity plans will be produced, maintained and tested.
- ICT security and Cyber Awareness training will be available to all staff.

2. Policy Objectives

2.1 Against this background there are three main objectives of the ICT Security Policy:

- to ensure that equipment, data and staff are adequately protected against any action that could adversely affect the organisation;
- to ensure that users are aware of and fully comply with all relevant legislation;
- to create and maintain within the organisation a level of awareness of the need for ICT security to be an integral part of the day to day operation so that all staff understand the need for ICT security and their own responsibilities in this respect.

3. Application

3.1 The ICT Security Policy is intended for all staff who are either controllers of systems or who are users and supporters of ICT systems or data. Users using ICT systems or data are subject to Albyn's IT Acceptable Use Policy and Social Media Policy.

3.2 For the purposes of this document the terms 'ICT' (or 'ICT systems'), 'ICT data' and 'ICT user' are defined as follows:

- 'ICT' (or 'ICT systems') means any device or combination of devices used for the storage or processing of data and includes: workstation (laptop, notebook, desktop PC), Smartphone, server or any other similar device;
- 'ICT data' means any information stored and processed within the ICT system and includes programs, text, pictures and sound;
- 'ICT user' applies to any employee, or other authorised person who uses the organisation's ICT systems and/or data.

4 Roles and Responsibilities

4.1 The ICT Security Policy relies on management and user actions to ensure that its aims are achieved. Consequently, roles and responsibilities are defined below.

4.2 Governing Body

4.2.1 The governing body has the ultimate corporate responsibility for ensuring that Albyn complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters. In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Chief Executive Officer.

4.3 Chief Executive Officer

4.3.1. The Chief Executive officer (CEO) is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the organisation's ICT Security Policy, as may be amended from time to time, is adopted and maintained across the group. He/she is also responsible for ensuring that any special ICT security measures relating to ICT facilities are applied and documented as an integral part of the Policy.

4.3.2. The day-to-day functions are delegated to the Director of Finance & Corporate Services, who will be supported in this task by the ICT Officer and the Organisation's contracted ICT services provider.

4.3.3. The CEO is responsible for ensuring that the requirements of the General Data Protection Regulation are complied with fully by the Group. This is represented by an on- going responsibility for ensuring that the:

- registrations under the General Data Protection Regulation are up-to-date and cover all uses being made of regulated data and;
- registrations are observed across the group.

4.3.4. In addition, the CEO is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy. This is particularly important with the increased use of computers and laptops at home. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened, specifically in relation to the General Data Protection Regulations.

4.4 Director of Finance & Corporate Services (DOF)

4.4.1. The DOF is responsible for the Group's ICT equipment, systems and data and will

have direct control over these assets and their use, including responsibility for controlling access to these assets and for defining and documenting the requisite level of protection.

4.4.2. The DOF will arrange for the administration of the practical aspects of ICT protection and ensure that various functions are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data. This task will be supported by the ICT Services Provider who will hold specific procedures in carrying out such duties.

4.4.3. In line with these responsibilities, the DOF will be the official point of contact for ICT security issues and as such is responsible for notifying the CEO and Chair of the Board of any suspected or actual breach of ICT security occurring within the organisation. The details of the suspected or actual breach will be reported through to the Board and made available to Internal Audit upon request. The DOF or CEO must advise the Audit Committee of any suspected or actual breach of ICT security pertaining to financial irregularity.

4.4.4. It is vital, therefore, that the DOF is fully conversant with the ICT Security Policy and maintains an up-to-date knowledge of best practice and follows the associated approved practices.

4.5 ICT Services Provider supported by the ICT Officer (ICTSO)

4.5.1. The ICTSO is responsible for maintaining, repairing and proactively supporting the ICT System so that it can meet the requirements of the ICT Security Policy.

4.5.2. The ICTSO will also monitor the ICT System for breaches of security and inform the DOF.

4.6 Users

4.6.1. Users are those employees or authorised users of Albyn who make use of the ICT system to support them in their work or duties. All users of the ICT systems and data must comply with the requirements of this ICT Security Policy. The Organisation has an Acceptable Use Policy which sets out the responsibilities of users of the ICT systems.

4.6.2. Users are responsible for notifying the ICTSO of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the CEO, DOF or Chair of the Board as appropriate.

4.6.3. Users are responsible for the equipment they use including:

- Physical security
- Security of data
- Their own passwords.

5 Management of the Policy

5.1 Sufficient resources should be allocated each year to ensure the security of the Organisation's ICT systems and to enable users to comply fully with the legal requirements and policies covered in this policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Board.

5.2 Suitable training for all ICT users and documentation to promote the proper use of ICT systems will be provided. Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data. A record of the training provided through to each individual user will be maintained by the HR Function. Development of the training programme will be the responsibility for the ICTSO and DOF.

5.3 In addition, users will be made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for ICT security and Data Protection.

5.4 To help achieve these aims, the relevant parts of the ICT Security Policy and any other information on the use of particular facilities and techniques to protect the systems or data will be disseminated to users.

5.5 The DOF must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that provide for continuity of ICT security when staff vacate or occupy a post. These measures as a minimum must include:

5.1.1 a record that new staff have been issued with, have read the appropriate documentation relating to ICT security;
5.1.2 a record of the access rights to systems granted to an individual user and their limitations on the use of the data in relation to the data protection registrations in place;
5.1.3 a record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment.

6 Physical Security

6.1 Location Access

6.1.1. Adequate consideration should be given to the physical security of rooms containing ICT equipment (including associated cabling). The server rooms should be locked to unauthorised access and have a controlled environment in line with system requirements.

6.1.2. The ICTSO must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks

might have.

6.2 Equipment siting

6.2.1. Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:

- devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
- equipment is sited to avoid environmental damage from causes such as dust & heat;
- users are instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained;
- users are instructed not to leave hard copies of sensitive data unattended on desks.

6.2.2. The same rules apply when accessing the ICT System or ICT data away from the Office environment, e.g. at a User's home or out on Albyn business.

6.3 Inventory

6.3.1 The DOF, in accordance with the Financial Regulations, shall ensure that an inventory of all ICT equipment is maintained including the details of equipment issued to each Albyn user.

7 Legitimate Use

7.1 The Organisation's ICT facilities must not be used in any way that breaks the law or breaches internal standards.

7.2 Such breaches include, but are not limited to:

7.1.1 making, distributing or using unlicensed software or data;
7.1.2 making or sending threatening, offensive, or harassing messages;
7.1.3 creating, possessing or distributing obscene material;
7.1.4 unauthorised personal use of Albyn's computer facilities.

7.3 Private Hardware & Software

7.3.1 Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on Albyn's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of any private software for Albyn

purposes must be approved and recorded by the DOF.

7.4 ICT Security Facilities

7.4.1 Albyn's ICT systems and data will be protected using appropriate security arrangements outlined in the rest of Section 7. In addition, consideration should also be given to including appropriate processing controls such as audit trails, input validation checks, control totals for output, reports on attempted unauthorised access, etc.

7.4.2 For new systems, it is recommended that such facilities be confirmed at the time of installing the system.

7.5 Authorisation

7.5.1. Only persons authorised by the ICTSO and in full compliance with the ICT policies, are allowed to use the ICT systems. The ICTSO will ensure the user is fully aware of the extent to which an ICT User may make use of the ICT System.

7.5.2. Failure to establish the limits of any authorisation may result in Albyn being unable to use the sanctions of the Computer Misuse Act 1990. Not only will it be difficult to demonstrate that a user has exceeded the authority given, it will also be difficult to show definitively who is authorised to use a computer system.

7.5.3. Access eligibility will be reviewed periodically, including remote access for support. In particular the relevant access capability will be removed when a person leaves the employment of Albyn. In addition, access codes, user identification codes and authorisation rules will be reviewed whenever a user changes duties.

7.5.4. Failure to change access eligibility and passwords will leave the ICT systems vulnerable to misuse.

7.6 Passwords

7.6.1. The level of password control will be defined by the ICTSO, including the possible use of "time out" passwords where a terminal/PC is left unused for a defined period.

7.6.2. **Passwords for staff users**

- Passwords MUST be a minimum of 8 characters, including a mix of letters (upper and lower case) and numbers.
- Passwords will be subject to a controlled expiry date at which point the user must provide a new password.

7.6.3. Passwords should be memorized, never shared and if stored separately should only be stored in encrypted form.

7.6.4. Passwords should protect access to all ICT systems.

7.6.5. A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur, such as:

- when a password holder leaves or is transferred to another post;
- when a password may have become known to a person not entitled to know it.

7.6.6. The need to change one or more passwords will be determined by the risk of the security breach.

7.6.7. Users must not reveal their password to anyone.

7.7 Security of the network

7.7.1. Only devices approved by the ICTSO should be permitted to be connected to the network, either through wired or wireless connectivity.

7.7.2. Where devices are connected to the network using wireless, the wireless network should be secure; as a minimum this should be done using WPA. Open Access Wireless Access Points must not be connected to Albyn's network.

7.7.3. Encryption is applied to wireless networks, encryption keys should be kept secure and remain the property of the ICTSO and must not be shared without written permission.

7.7.4. Mobile devices may with permission to connect to the network but in full compliance with the ICT policies and this permission may be withdrawn at any time. The ICTSO will inform the owner/user that if a mobile device connects to the internet connection, then the device's online activity will be monitored and logged by the Organisation.

7.8 Encryption

7.8.1. All devices that have access to data attached to the ICT System are fully encrypted Devices subject to encryption may include:

- Laptops
- Smartphones
- Desktop PC's

7.8.2. Where technology prevents the use of encryption then any sensitive data should not be stored directly on these devices.

7.9 Filtering of the Internet

7.9.1 Access to the internet for staff should be filtered using an approved system.

7.9.2 It is the responsibility of the ICTSO to monitor the effectiveness of filtering and report issues to the DOF and the Organisation's Internet Service Provider.

7.9.3 Where breaches of internet filtering have occurred, the ICTSO should inform the DOF and assess the risk of continued access.

7.10 Backups

7.10.1 In order to ensure that essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the ICTSO.

7.10.2 Data essential for the day to day running and management of the Organisation will be stored on the Organisation's network. Supplementary backups are replicated though DataBarracks.

7.10.3 Backups contain data that must be protected and should be clearly identified as to what they are and when they were taken.

7.10.4 Instructions for recovering data or files from backup should be fully documented and should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

7.11 Operating System Patching

7.11.1 The ICTSO will ensure that all devices defined as part of the ICT System are patched up to date according to those releases distributed by the manufacturers of the operating systems.

7.12 Virus Protection

7.12.1. Albyn will use appropriate Anti-virus/Anti-malware software for all ICT systems, which will be deployed and operated by the ICTSO.

7.12.2. All Users should take precautions to avoid malicious software that may destroy or corrupt data.

7.12.3. Albyn will ensure that every ICT user is aware that any device in the ICT system (PC, laptops, smartphone) with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the ICTSO who must take appropriate action, including removing the source of infection.

7.12.4. Any third-party laptops/mobile devices and mobile storage not normally connected to the network must be checked by the ICTSO for viruses and up-

to-date anti-virus software before being allowed to connect to the network.

7.12.5. ICTSO will ensure that up-to-date anti-virus signatures are applied to all servers and that they are available for users to apply, or are automatically applied, to PCs or laptops.

7.13 Disposal of Waste

7.13.1. Disposal of waste ICT media will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.

7.13.2. The General Data Protection Act (GDPR) requires that adequate mechanisms be used when disposing of personal data.

7.14 Disposal of Equipment

7.14.1. The General Data Protection Act requires that any personal data held on a part of the ICT system subject to disposal will be destroyed.

7.14.2. Prior to the transfer or disposal of any ICT equipment the ICTSO must ensure that any personal data or software is removed from the device if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the General Data Protection Act (GDPR) to be met. Normal disposal requirements as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.

7.14.3. It is important to ensure that any copies of software remaining on a device being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently. Albyn will maintain a regularly updated asset register of licenses and should indicate when licenses have been transferred from one part of the ICT system to another.

7.15 Repair of Equipment

7.15.1 If a device, or its permanent storage (usually a disk or solid state drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on other media for subsequent reinstallation, if possible. Albyn will ensure that third parties are currently registered under the General Data Protection Act (GDPR) as personnel authorised to see data and as such are bound by the same rules in relation to not divulging the data or making any unauthorised use of it.

8 Security Incidents

8.1 All suspected or actual breaches of ICT security shall be reported to the ICTSO or the DOF in their absence, who should ensure a speedy and effective response to be made to an ICT security incident, including securing useable evidence of breaches and evidence of any weakness in existing security arrangements. They must also establish the operational or financial requirements to restore the ICT service quickly.

8.2 It should be recognised that Albyn and its officers may be open to a legal action for negligence if a person or organisation should suffer as a consequence of a breach of ICT security within the Organisation where insufficient action had been taken to resolve the breach.

9 Acceptable Use Policy

9.1 Albyn's Acceptable Use Policy applies to all staff, and other users who use either or both of these facilities. The policy covers the use of Email, the Internet, services accessed through the Internet and local file and network usage. The conditions of use are explained in the policy. All users accessing these facilities must be issued with a copy of the Acceptable Use Policy and other relevant documents.

10 Personal Use

10.1 Albyn has devoted time and effort into developing the ICT Systems to assist users with their work. It is, however, recognised that there are times when users may want to use the Systems for non-work-related purposes, and in recognising this need the Organisation permits users to use the Systems for limited personal use.

10.2 ICT systems must not be used for personal use during working hours. Users must not allow personal use of systems to interfere with day-to-day duties. Any non-job related use of the systems during working hours may be subject to disciplinary action.

10.3 Users must not utilize software for personal use unless the terms of the licence provides permission.

10.4 Use of Albyn ICT systems for personal use must always be in compliance with the Acceptable Usage Policy which is available on the staff Intranet

11 Disciplinary Implications

1

11.1 Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the Computer Misuse Act 1990 and may lead to prosecution of the Organisation and the individual(s) concerned and/or civil claims for damages.

END.