ARK HOUSING ASSOCIATION LTD (ARK)

POLICY REF: G15
POLICY REF: G09
PROCEDURE REF: G46

Version 1 – February 2019

ICT SYSTEMS SECURITY PROCEDURE

1. Introduction

1.1 Background

ARK has an obligation to its members to clearly define requirements for the use of its information and communications technology (ICT). This is so that users of ICT facilities do not unintentionally place themselves, or the Association, at risk of prosecution, by carrying out computer related activities outside the law.

In addition, although the bulk of information held is intended to be openly accessible and available for sharing, certain information (key data and information) has to be processed, handled and managed securely and with accountability. Legislation is again the key driver of this requirement, but it is also derived from the criticality and sensitivity of certain information where loss of accuracy, completeness or availability could prevent the Association from functioning efficiently, or where disclosure could damage the Association's reputation. Unless policy is in place to stipulate control requirements for such information, there is an increased risk that security breaches will be suffered, potentially resulting in a wide-range of adverse consequences.

1.2 Purpose and Scope

Information plays a major role in supporting ARK's strategic and administrative activities. The purpose of the policy is to provide a framework for protecting:

- The Association's ICT infrastructure;
- Key data and information;
- Those who have access to or who administer ICT facilities;
- Individuals who process or handle key data and information.

The procedure is designed to provide protection from internal and external security threats, whether deliberate or accidental by:

- Defining the procedure for the protection of the Confidentiality, Integrity and Availability (CIA **1**) [1]of its' key data and information; Establishing responsibilities for information security;
- Providing reference to relevant documentation and policies.

[1] CIA is the industry standard abbreviation (ISO 27002) for Confidentiality, Integrity and Availability, the required components for information security

1.3 Objective

Information Security controls are designed to protect all those associated with ARK and The Association's reputation through the preservation of CIA:

- Confidentiality - knowing that key data and information can be accessed only by those authorised to do so;
- Integrity - knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and,
- Availability - knowing that the key data and information can always be accessed.

ARK is committed to protect both its members and its key data and information and to deploy controls that minimise the impact of any Security Incidents.

1.4 Applicability

The procedure applies to the following categories

- All full-time, part-time, relief and temporary staff employed by, or working for or on behalf of The Association;
- Contractors and consultants working for or on behalf of The Association;
- All other individuals and bodies, including Board Members, who have been granted access to The Association's ICT systems and/or key data and information.

Any breach of these procedures will be dealt with in terms of our disciplinary policy and procedures, or under the Board Members Code of Conduct, as appropriate. Serious breaches of these procedures will be considered gross misconduct in accordance with our disciplinary policy and procedures.

It is the personal responsibility of each person to whom the procedure applies to adhere with its requirements.

This procedure should be read in conjunction with the Computer System Security, Email & Internet Policy(G15), Openness & Confidentiality policy G13, the Business Continuity policy G09 and related procedures.

2. Organisational Security

2.1 Security of Third Party Access

Access to The Association's information processing facilities by third parties is controlled by ICT.

3. Asset classification

Information assets are categorised and recorded to enable appropriate management and control.

3.1 Inventory of Assets

Inventories of information assets, including hardware, software and key data are developed and maintained by ICT.

3.2 Protection of Key Data and Information

Key data and information will be classified and managed in accordance with the General Data Protection Regulation

4. Personnel Security

Through the ARK induction process all employees must signoff that they have read and understood the Staff Code of Conduct, the Computer System Security, Email & Internet Policy (G15) and the Openness and Confidentiality Policy (G13) prior to gaining access to ARK systems to reduce the risks of, theft, fraud or malicious misuse of facilities.

4.1 Personnel Screening

Employee reference checking, Disclosure Scotland and PVG (Protection of Vulnerable Groups) checks are carried out prior to commencing employment in accordance with the Recruitment Policy, to minimise the likelihood of personnel, who pose a security risk, being employed in posts involving key data and information, such as those concerned with financial or personnel related data.

4.2 Confidentiality undertaking

All members of staff are bound by the Openness and Confidentiality Policy (G13) to protect confidential information in accordance with The Association's standard terms and conditions of employment.

4.3 Employee Responsibilities

Employees will be informed of their information security responsibilities during the induction process.

4.4 Responding to Security Incidents

4.4.1 Suspected Security Weaknesses

Those using or administering the ICT facilities must not try and prove any suspected or perceived security weakness. The exception to this rule is where support staff have been granted a specific policy exemption which allows them to do so as part of their role.

4.4.2 Reporting Security Incidents

All actual and suspected security incidents are to be reported to the Head of ICT.

4.4.3 Network Isolation and Reconnection

Any computer that is perceived to be placing the integrity of the network at risk will be disconnected at the network boundary. Subsequent reinstatement will only be permitted once the integrity of the system has been verified.

4.4.4 Security Incident Management

Events that are regarded as being 'security incidents' will be defined, and processes implemented to investigate, control, manage and review such events, with a view to preventing recurrence.

All incidents are logged and maintained in the ICT Helpdesk log. Each incident is investigated and compared against the relevant system monitoring tools or logs depending on the nature of the incident. A full review will be undertaken to determine if there are any weaknesses in the security strategy and appropriate action deployed to prevent further incidents or patch identified flaws in software or procedures.

5. Physical and environmental security

Controls will be implemented as appropriate to prevent unauthorised access to, interference with, or damage to, information assets.

5.1 Physical Security

Computer systems and networks are protected by suitable physical, technical, procedural and security controls.

Access to all core, networking and Datacentre equipment in the infrastructure are situated either in secure rooms and/or secure cabinets. Access to all of these areas is restricted to ICT and permission to access these areas out with ICT staff must be obtained from ICT.

File servers and machines that hold or process high criticality, high sensitivity or high availability data are located in physically secured areas.

Access to facilities that hold or process high criticality, high sensitivity or high availability data is controlled.

The Datacentre has further environmental security features that reflect the critical nature of the equipment and data held within this area. This room is temperature controlled by air conditioning, which is regularly maintained by an external supplier. All server, storage and networking equipment are further protected by a dual UPS (uninterrupted power supply) system to ensure uptime and failover in the event of an electrical outage.

6. Operations Management

6.1 Virus Protection

Anti-Virus technology is implemented to prevent the introduction and transmission of computer viruses both within and from outside the Association. This extends to managing and containing viruses should preventative measures fail. Real time monitoring identifies / alerts of any issues – should a potential threat arise this will either be automatically deleted, quarantined or blocked dependant on the nature of the threat that was identified by virus protection software.

6.2 Security Patches, Fixes and Workarounds

ICT is responsible for the day to day management of systems and to ensure that security patches, fixes and workarounds are applied in accordance with the agreed schedule. This is scheduled on a weekly basis and recorded in the Change Management Log with any issues identified being addressed and also documented in the Change Management Log. The Change Management log is a repository for all major system changes to be logged and documented. This log provides a history of change and the responsible personnel and is an invaluable tool in troubleshooting issues that occur and attempting to identify the source of the problem.

6.3 Vulnerability Testing

External Penetration Testing will be scheduled annually by ICT.
Penetration Testing provides effective testing and reporting that details discovered vulnerabilities according to risk, provides descriptions of technical findings and provides mitigation advice for all identified vulnerabilities.

6.4 System, Application and Data Backup

All critical systems are managed in accordance with the following Backup procedure - see below:

Once logged into the network, either on the physical network or via Citrix from the services, the files, emails and application data that are accessed are stored on network file servers. All files and all servers on the network located at the Priory are backed up every night of the week.

ARK uses a backup software product to perform daily system backups of all servers on the network and provide data retention and writes these backup images to a Network Attached Storage (NAS) device. This device acts as the primary storage device for backups. Depending on the nature of the server being backed up will determine the number of backup iterations that are stored on the backup NAS device. Servers that contain regularly changing data will have iterations that go back 6 months; servers that are mostly static in nature will have backup iterations of 3-4 weeks. These daily backups are copied to external drives (secondary storage devices) on a rota system to provide adequate cover for the server backups on the NAS. An external drive is attached to the NAS each weekday and removed the following day, the backup is set to run automatically each night, out with office hours. The backup copy is also set to run automatically every night to the external drives.

Each daily external drive is locked in secure storage, and the weekly drive is taken offsite every Monday and kept offsite till the following Monday. The scheduled quarterly drives are stored in the fire safe on the second floor and are replaced on an annual basis.

The backup software can be used to restore data and whole servers in case of accidental deletion, corruption or system failure. Item or system restores should be processed from the primary storage device.

Secondary storage drives provide additional cover to the data stored on the NAS device and can be used to restore data in the same manner as the primary storage device should the primary storage device be unavailable for any reason or for Disaster recovery.

ARK Housing has a Business Continuity process that utilises this backup software to replicate the entire virtual server infrastructure every night of the week to an external supplier.

6.5 System Monitoring

System Monitoring encompasses management tools, manual scheduled processes and system alerts. These tools and scheduled processes augment and enable the daily proactive nature of the ICT department. Daily system checks for updates, patches, security vulnerabilities and industry wide recommendations, have to be verified, scheduled and implemented.

6.5.1 Management Tools

The Anti-Virus System Management console is responsible for much more than just the management of Anti-virus software. This facility reports the real-time status of:-

- The virus condition of all Microsoft Windows devices on the network.
- The online status of all Windows Devices
- The security status of all windows devices pertaining to patch levels

- The security status of firewall settings for all Windows Devices
- The health status with regards to disk space, memory and CPU resources of all Windows Devices

The Hypervisor Management is responsible for management and configuration of all virtual servers.

- Installation/configuration and management of the VMware hosts
- Installation/configuration and management of the VMware virtual servers
- Patch management of all hardware and software components
- Monitoring status of all CPU/memory/disc activity and Network statistics of all VMware virtual servers

The Network Analyser is used to monitor the Network infrastructure of all cisco switches

- Real-time network monitoring of all interconnectivity and switch status
- Patch management of all cisco switches
- Critical reporting of all major outages or network issues

Backup & Replication Management console software manages our backup and replication processes.

- The results of every backup job for every server are reported and emailed to ICT
- The results of every replication job for every server are reported and emailed to ICT.

Webfilter Portal is responsible for the monitoring and scanning of all Internet activity

- All critical security issues such as malware are email to ICT
- The “dashboard” feature display current and recent web activity highlighting risks and usage statistics.
- Reports on historical usage/top users/top sites/infected and blocked sites.

The External E-Mail Anti-Spam/Anti-Virus Portal is our management and configuration tool for all external Email in and out of the organisation.

- All critical security issues such as viruses are emailed to ICT.
- Real-time usage of all emails in and out of the system and their delivery status can be monitored.
- Allow and block list are configured.
- Reports on top senders/top receivers of email.
- Reports on viruses detected and whether quarantined or destroyed.
- SPAM reporting and configuration

6.5.2 Manual Monitoring Processes

The weekly maintenance window utilises the planned downtime to:-

- Patch all windows servers
- Restart servers on a scheduled maintenance.
- Clear down user profiles
- Install/Upgrade software components
- Patch the Hypervisor environment.
- Patch the firmware levels of the firewalls, switches, webfilters and SANs

6.5.3 System Alerts

All Hardware components configured to Email alert ICT of any critical change in status or outage. These devices include:-

- The Hypervisor host servers
- The Storage Area Network.
- The Webfilter Portal
- The Core network switches
- The Corporate Firewall
- All the above mentioned System Monitoring tools.

7. Detailed descriptions

Adding and removing staff/ other authorised individuals from the ARK network

a) <u>All staff or other Authorised Individuals</u>

7.1 To add all new staff (with the exception of Support Workers see 7.2.1), non-ARK staff working for other group companies or someone contracted from another organisation ('authorised individual') who have been authorised to access the ARK network by the relevant ARK manager or director, to the system, the line manager or relevant ARK manager will complete a New ICT User Form (Appendix 1) and forward this by email to the ICT team 1 week before the employee/ authorised individual's start date. ICT team will issue a 'user identity' (login ID) and the required password(s) to the line manager or relevant ARK manager.

7.2 The line manager/ relevant ARK manager will ensure that new staff or authorised individuals have read this procedure and signed the relevant induction documentation **before** they issue the user identity and password(s).

7.2.1 New Care & Support (Support Worker) staff will be issued with a password only as they will be accessing existing accounts on the system. The line manager will ensure that new staff have read this policy and signed the relevant induction documentation **before** they receive their password.

7.3 For Staff/ authorised individuals ceasing employment or no longer requiring access to the ARK network the relevant line manager will complete an ICT User Leaving Form (Appendix 3). This will be passed (via the HR department for ARK Staff) to the ICT team prior to the effective leaving date (i.e. the date when the staff member actually stops working at ARK, which may be before their last Pay date). On or as soon as possible after their leaving date their account will be deactivated by ICT. ICT will delete the individual's details from the system one month from their leaving date unless the relevant manager makes a request to retain this data for a longer period of time.

When Care and Support (Support Workers) staff cease employment, or move to different service, the manager will ensure that the password of the relevant account shared by service staff is changed.

b) <u>Temporary staff</u>

7.4 The relevant manager will be responsible for ensuring that any temporary, freelance or consultancy staff has the required competence before they are allowed access to ARK's computer systems.

7.5 Visiting guests (e.g. freelance or consultancy staff, auditors etc.) requiring Wi-Fi access will be required to complete the Guest Wi-Fi use form (Appendix 5).

7.6 For further details of the processes for adding and deleting staff to the system see the procedures supporting this policy.

c) Members of the Board

7.7 Members of the Board will be responsible for ensuring that any equipment that they use to access and/or process ARK or group company related data is subject to appropriate virus and password protection.

7.8 Members of the Board will be responsible for ensuring that they back up any information pertaining to ARK at regular intervals, onto a suitable secure storage device, the ICT team can advise if required.

7.9 When a Member of the Board ceases their involvement with ARK, they will be required to delete or return all ARK or group company related data to the relevant department within ARK.

User identity and passwords

7.10 Only the ICT team will have the authority to issue a 'new user identity' (login ID) and an initial password for a new account.

7.11 Following issue of their login ID and initial password, staff will be advised:

- To ensure that their initial password is changed ; staff will be prompted to change their password at first login;
- All passwords are subject to a minimum complexity format and uniqueness state (same password cannot be re-used at a later date);
- That their password is confidential and must not be written down anywhere that could be accessible by others and should not be disclosed to any unauthorised person;
- Not to log into the network with any login ID or password other than the one issued to them, **except when** authorised to do so in advance for specific purposes by the relevant manager;
- If staff suspects that anyone else may know their password they should change their password immediately.

7.12 To maintain security, staff and other authorised individuals will be required by the system to change their login passwords every 42 days.

ICT hardware and software

7.13 All new ICT hardware and software (including mobile phones and removable storage devices) will be ordered by the ICT team in accordance with current procurement procedures, to ensure that the required standards are maintained and that the ICT asset register is kept up to date.

7.14 ARK employees should only use ARK issued hardware (including removable data storage devices such as USB memory sticks etc.) when conducting ARK business. The only exceptions to this will be as set out in section 7.15 below.

7.15 Non ARK Issued hardware such as employees' own personal computers or laptops, will only be used in connection with ARK work with the prior approval of the relevant Line Manager and/or the Head of ICT. Such work will only be undertaken by employees through accessing ARK's secure Citrix infrastructure. Under no circumstances will ARK related work be saved by ARK staff onto hard drives, personal laptops/computers, or any other non-ARK supplied storage medium.

7.16 Members of the ARK Board of Management will be permitted to use their own personal computers, laptops, mobile phones or tablets in connection with ARK business, on the basis that Board Members will take responsibility for ensuring that ARK or group company data is secure at all times,

password protected if necessary, and that such data is reviewed at regular intervals and deleted when no longer required. Board of Management Members wishing to dispose of hardware upon which ARK data has previously been saved should ensure that the hardware is securely disposed of, including full data wiping. Guidance can be sought from ARK's ICT team if required.

7.17 Further guidance on storing ARK related work on ARK issued removable data storage devices such as USB memory sticks etc. can be found at section 7.21.

7.18 All software to be used on ARK's computers and laptops will be approved by the Head of ICT and licensed to the specified user. No software may be down loaded from the internet without the prior approval of the Head of ICT. Unauthorised copying of proprietary software is a breach of the Copyright Act and will be a disciplinary offence.

7.19 All major software upgrades will be appropriately controlled and tested through a managed process before live implementation.

Developing applications

7.20 Staff and other authorised individuals who propose to develop small applications such as a database, spreadsheet or training application will ensure that they comply with this procedure, and in particular that they:

- Only develop such applications where there is a business reason for doing so;
- Comply at all times with the requirements of the General Data Protection Regulation;
- Do not expose themselves or ARK to adverse publicity, litigation or penalties by using software for which they have no licence to develop an application;
- Fully test any application before using it in a live environment;
- Put in place satisfactory security features to prevent misuse of the software and data;
- Develop adequate back-up procedures to protect the software and data.

Care and security of equipment, software and data

7.21 All staff and other authorised individuals will ensure that they take appropriate care of all hardware and software they use, including that of service users, to prevent loss or damage to the system and any applications and/or data held on it. The care and security measures will include:

- All hardware will be labelled by ICT with an identification number/serial number (labels **must not** be removed – if labels are worn/damaged please report to ICT);
- Hardware should not be tampered with (this includes mobile phones);
- Any ARK supplied equipment which is lost or stolen should be reported as soon as possible to the relevant line manager and ICT team;
- To prevent unauthorised access by others, staff will 'lock' their computer when leaving their workstation, and ensure they log out and switch off their computers when leaving work each day;
- Group policies are in place for Citrix access connections and user laptops to ensure that all devices / connections are locked after 15 minutes of inactivity
- Those using ARK laptops will ensure that these are always left in a secure location and not unattended particularly when in public places (e.g. train stations etc.), and where possible that they are placed in lockable secure storage overnight;
- Every effort should be made to store any confidential/sensitive data on the ARK network. Where this is not possible an encrypted mobile device supplied by ICT team **must** be used;
- All removable data storage devices such as CD's, USB memory sticks etc. will be held in secure lockable storage;

- Removable data storage devices (USB Memory Sticks) will be supplied by ICT on request, and will be encrypted for security purposes;
- Any confidential, personal or sensitive information or data relating to service users, tenants, employees or contractors, as set out in ARK's Openness and Confidentiality Policy and Data Protection Procedure will only be saved out with the ARK network removable storage with the prior agreement of the relevant member of the Leadership Team, Data Protection Officer and ARK's Head of ICT. In such cases, even if consent is obtained, such data will only be saved on ICT supplied encrypted removable storage devices;
- Where staff have the need to process ARK data on ARK issued laptops they should ensure that they back up the information at regular intervals onto a secure storage device (supplied by ICT), and that this is held separately in secure storage;
- Laptops will be subject to regular audit and maintenance by the ICT team;

For Board Members please see section 7.16

Confidentiality

7.22 All staff and other authorised individuals will ensure that they handle all the information they have access to in strict confidence, and that in particular they comply with the requirements of the General Data Protection Regulation, with our Openness & Confidentiality policy ref: G13 and our Data Protection procedures ref: G48.

Disposal of surplus hardware

7.23 Computer equipment that is no longer required will be identified by the Head of ICT, who will ensure that all data is deleted to ensure that no sensitive information is passed on to unauthorised persons.

7.24 Disposal will be carried out in accordance with the Disposal of Assets procedure ref: F22. Following disposal the Head of ICT will liaise with the Head of Finance/Finance Business Partner to update the asset register.

8.0 Implementation & Review

8.1 The Senior Leadership Team (SLT) is responsible for ensuring that this procedure is implemented throughout the organisation.

8.2 All Directors and Managers will be fully aware of the content of this procedure and ensure that it is followed by the staff they are responsible for.

8.3 All staff and Board members must ensure that they are familiar with the requirements of this procedure, and that they do not knowingly breach this policy.

8.4 The relevant line manager is responsible for ensuring that each new employee receives a copy of this procedure and that Induction documentation is completed timeously.

8.5 The Head of ICT is responsible for advising the Leadership Team on all technical issues which may affect this procedure, so that they are dealt with promptly.

8.6 The Head of ICT will ensure that this procedure is reviewed at least every 3 years.

Reviewed by the SLT: February 2019

Next review due by: February 2022

Appendix 1

NEW ICT USER FORM

Upon completion of this form an account will be created for the named user enabling email and internet access as well as access to any systems or directories specified.

Line manager: Complete this form and email it to the ICT team **at least 1 week** before the date a new employee/ new authorised user starts/ requires access. Ensure that the Computer System Security policy and procedure have been given to the new employee/ user, and that they have read and understood them and signed the statement, **before** receiving their login ID and password(s).

NEW USER DETAILS				
Name:				
Location:				
Post title:				
Commencement date:				
End Date (If Temporary):				
Access required to: *(tick if required)*	IBS Housing		IBS Finance	
	HR/Payroll			
Directories:	Admin		Housing	
	Finance		New Finance	
	Personnel		Maintenance	
General Drive or Projects Drive: *Please list folders for **full** access*				
Line Manager's name:		**Date:**		

For ICT use only

RECORD OF ACCOUNT OPENING			
Date account set up:		**User login ID:**	
Capita login ID (if required):			
HR/Payroll login ID (if required):			
ID & password passed to line manager on:			
Completed by:		**Date:**	

Appendix 2

ICT USER LEAVING FORM - ALL STAFF OR OTHER AUTHORISED INDIVIDUALS

All staff/ authorised individuals with access to ICT equipment who are terminating their employment with ARK/ no longer require access must complete this ICT User Leaving Form. Please complete the 'User Details' section then pass to the HR department who will forward it to the ICT team. In the case of a non ARK ICT user the completed form can be forwarded directly to the ICT team.

USER DETAILS	
Name	
Username	
Date of leaving ARK/ No longer requiring access	
Line Manager Name	
I have returned all software, data and ICT equipment belonging to ARK Housing Association that has been issued to me and/or been in my possession.	
Date	
Employee/ Authorised individual's signature	

For ICT use only

RECORD OF ACCOUNT CLOSURE			
Line Manager contact?		**Y/N**	
Specific user data requirements			
Capita account disabled			
Hardware log updated			
AD account and Exchange deleted			
Personal Directory and User Folders deleted			
Completed by:		**Date:**	

Appendix 3

GUEST Wi-Fi USE FORM

By obtaining Wi-Fi internet access utilising ARK's corporate network I agree to comply with the terms and conditions of ARK's Acceptable Use Statement (AUS).

Acceptable Use Statement

All users of the Wi-Fi System must comply with this Acceptable Use Statement (AUS). This AUS is intended to prevent unacceptable uses of the internet. ARK may remove, block, filter or restrict by any other means any materials that, in our sole discretion, may be illegal, may subject ARK to liability or may violate this AUS. Such accessing, downloading and/or circulation by authorised individuals will result in access to the ARK network being terminated, and will be reported by the relevant ARK manager to the individual's line manager either within ARK or in their own organisation. ARK may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. Violation of this AUS may result in the suspension or termination of your access to the Wi-Fi System.

On completion this form must be handed to ICT (by the relevant ARK manager) before you will be granted Wi-Fi access.

Signed: _____

Name: _____
[Please print]

Company: _____

Date: _____

The above Acceptable Use Statement is a snapshot of the ARK staff terms of Internet Access Use – the complete relevant passage from this policy is available on request.