# ICT Security Procedure

## Procedure Reference Number: IT02a

| | | | |
|---|---|---|---|
| **Effective Date:** | May 2025 | **Review Date:** | May 2028 |
| **P&P Review Group Approval Date:** | April 2025 | **Related Policy** | IT02 |
| **Owner:** | Head of ICT Strategy & Development | **Department:** | ICT |
| **Issued To:** | ☐ Board of Management<br>☐ All Staff<br>☐ ET/LT<br>☐ Head Office Managers<br>☐ C&S Managers<br>☒ Department/Other:<br>____ICT_____ | **Method of Delivery:** | ☒ Annual Declaration<br>☐ LearnPro Individual Sign Off<br>☐ Board Portal |
| **Stakeholder Consultation** | ☐ All Staff<br>☐ Customer Engagement<br>☐ Union<br>☐ Employee Voices Group<br>☐ Head Office Managers<br>☐ C&S Managers<br>☐ Department/Other:<br>_____ | This procedure will be reviewed every 3 years from the date of implementation or earlier if deemed appropriate. If this procedure is not reviewed within the above timescale, the latest approved procedure will continue to apply. | |

**Version Control**

| Date | Owner | Version | Reason for Change |
|---|---|---|---|
| Feb-25 | Head of ICT Strategy & Development | 1.0 | Material review of existing ICT policies and procedures to reflect changes to Ark's ICT operating environment since the previous policy (G15) was reviewed in May 2021 |

**Summary of changes**

| Section | Change |
|---|---|
| All | Previous procedure included a mix of ICT specific detail and wider user detail ('do's and don'ts) throughout; the latter has now been moved out of this procedure and into Ark's new IT01 Acceptable Use policy. This procedure now focuses on key ICT actions that are required to ensure Ark maintains a secure ICT environment. |
| | |
| | |

# Contents

# 1.0 Introduction

Ark has an obligation to its users to clearly define requirements for the use of its Information and Communications Technology (ICT). This is to ensure that users of ICT facilities do not unintentionally place themselves, or Ark, 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 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 Ark from functioning efficiently, or where disclosure could damage Ark's reputation or lead to legal proceedings.

# 2.0 ICT Security

## 2.1 Objective

Information security controls are designed to protect all those associated with Ark and the Group's reputation through the preservation of:

- 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 protecting both its staff and all authorised users, and its key data and information and to deploy controls that minimise the impact of any Security Incidents.

The Head of ICT Strategy & Development is responsible for advising Ark's Senior Leadership Team on all technical issues which may affect this procedure, so that they are dealt with promptly.

## 2.2 System Security Incidents

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

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

Any computer/system 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.

All system security incidents will be logged and maintained in the ICT helpdesk log. Each incident will be 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.

## 2.3 ICT Hardware

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

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 are:

- Frontline Care & Support employees who have indicated a preference to use their own device rather than an Ark provided tablet, and who have agreed to have mobile device management software installed on their personal device;
- Board of Management members who access Ark documentation via Microsoft 365.

## 2.4 Software

All software to be used on Ark's devices will be approved by the Head of ICT Strategy & Development and licensed to the specified user. No software may be downloaded from the internet without the prior approval of the Head of ICT Strategy & Development. Unauthorised copying of proprietary software is a breach of the Copyright Act and will be dealt with through Ark's Disciplinary Policy & Procedures.

All major software upgrades will be appropriately controlled and tested through a managed process before live implementation by authorised ICT staff.

## 2.5 New User Identify and Passwords

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

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

- To ensure that their initial password is changed; staff will be automatically 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 it immediately;
- Passwords should be created randomly to maximise security; passwords should not be created which form a pattern that ex-staff would be able figure out (e.g. month and year or service name with numbers after it);
- To maintain security, staff and other authorised individuals will be required by the system to change their login passwords every 180 days.

## 2.6 Disposal of Surplus Hardware

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

Where possible (and safe to do so), Ark will look to gift equipment to other charitable organisations. If this is not feasible, devices will be recycled or disposed of in an appropriate environmental manner.

Following disposal, the Head of ICT Strategy & Development will liaise with the Head of Finance to update the fixed asset register.

### 2.7 Virus Protection

Ark will ensure appropriate Anti-Virus technology is implemented at all times, to prevent the introduction and transmission of computer viruses both within and from outside Ark. This extends to managing and containing viruses should preventative measures fail.

Real time monitoring will identify/alert Ark's ICT team 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.

### 2.8 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 documented in the Change Management Log.

The Change Management log is a repository for all major system changes to be logged and documented, this provides a history of change and the responsible personnel. It is an invaluable tool in troubleshooting issues that occur and attempting to identify the source of the problem.

### 2.9 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 mitigation advice for all identified vulnerabilities.

The results of penetration testing will be reported to the Board of Management as part of the annual Business Continuity report.

## 3.0 System, Application, and Data Backup

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

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 servers on the network located at Head Office 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.

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 taken offsite. The drives are brought back when required.

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 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 partner as per the terms of the contract. In the event of a full Disaster Recovery event, the latest offsite external storage drive should be delivered to the external partner to provide extra resilience to the recovery procedure.

# 4.0 System Monitoring

## 4.1 Overview

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 must be verified, scheduled, and implemented.

## 4.2 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 HP switches:

- Real-time network monitoring of all interconnectivity and switch status.
- Patch management of all HP 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.

## 4.3 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.

## 4.4 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.

## 5.0 Related Documents

Related forms, records or systems used are referenced throughout the procedure. Further detail on monitoring requirements can be found within procedure IT02b – ICT Systems Monitoring and Patching.

## 6.0 Training & Monitoring requirements

### 6.1 Training

ICT staff will have training appropriate to their needs and to the needs of the organisation as identified on their individual learning plans. Ark will ensure that relevant employees have an awareness of this policy and receive adequate training to enable them to effectively fulfil their roles and ensure Ark's ICT infrastructure remains safe and resilient.

### 6.2 Monitoring

System monitoring activity is noted throughout this procedure.