ICT Systems Monitoring and Patching Procedure

Procedure Reference Number: IT02b

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 ☐ All Staff ☐ ET/LT ☐ Head Office Managers ☐ C&S Managers ☒ Department/Other: ____ICT_____	**Method of Delivery:**	☒ Annual Declaration ☐ LearnPro Individual Sign Off ☐ Board Portal
Stakeholder Consultation	☐ All Staff ☐ Customer Engagement ☐ Union ☐ Employee Voices Group ☐ Head Office Managers ☐ C&S Managers ☐ Department/Other: _____	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	Remove reference to 'The Priory', replaced with 'Head Office'
Appendix 1 & 2	Removed reference to Capita products as no longer in use

Contents

1.0 Introduction 3
1.1 Overview 3
1.2 Scope 3
1.3 Responsibilities 4
2.0 ICT Systems Monitoring and Patching 4
2.1 Requirements 4
2.2 Software 4
2.3 Patching and Remediation 5
2.4 Windows Updates 5
2.5 End-User Devices 5
2.6 Server OS Patching 5
2.7 Security Monitoring 6
3.0 Solutions 6
3.1 Wi-Fi Monitoring 6
3.2 Emerging threats 6
3.3 Penetration Testing 6
3.4 Web Access Control 7
3.5 Windows Anti-Virus 7
4.0 Related Documents 7
5.0 Training & Monitoring requirements 7
5.1 Training 7
5.2 Monitoring 7
Appendix 1 Daily Checklist 8
Appendix 2 Weekly Checklist 9

1.0 Introduction

1.1 Overview

The security and availability of ICT services and systems provided by Ark are essential to support the organisation to operate effectively. To this end, a resilient, tested and thorough monitoring and security / functional patching procedure is essential. Monitoring must be carried out locally, or by a third party, in a manner that is reliable, resilient and workable i.e. it is has a minimal “false positive” notifications to ensure confidence and a valid response.

To ensure security, all systems must be kept to an acceptable systems’ patch level. This requires both manual attention to vulnerabilities that are made public, and patches of a high and/or critical security nature being identified and applied within an acceptable time period. This is especially important on those systems exposed to internet access. The exposure to external threats must be regularly assessed and reviewed to ensure that any external “attack profile” is minimised.

1.2 Scope

This procedure applies to Ark’s ICT department and third parties that host or provide ICT services to Ark. The ICT Department, alongside any third party, will be responsible for the instigation and maintenance of all monitoring.

This procedure will outline the requirements to ensure:

- a reliable and secure ICT platform;
- that all systems are monitored to the necessary level; and
- that all systems are kept at a secure systems patch level requisite to their purpose and audience.

Information and systems’ security and availability can only be assured and assessed by the consistent and application of qualitative monitoring and the application of security remediation. Where this is lacking, systems are prone to failure due to lack of insight into performance, capacity, vulnerability and availability. The result of these failures will lead to systems’ downtime, data loss, data theft or corruption.

1.3 Responsibilities

It is the responsibility of the ICT department, partners, and contractual third parties that host or provide ICT services to Ark to ensure that all systems are monitored to a standard that will provide insight into:

- Failure of a system or service;
- Impending failure due to measurable parameters;
- Performance problems; and
- Security failures and vulnerabilities.

The system emplaced to perform this must be reliable and all fault reporting mechanisms must be self, or remotely, monitored to ensure reliability.

2.0 ICT Systems Monitoring and Patching

2.1 Requirements

Set out below are the minimal requirements for patching, monitoring and remediation for infrastructure systems. Any production system or service made available to Ark's end users must comply with these requirements.

A full list of all checks that are carried out on a weekly and daily basis can be found in the ICT only drive in the Daily Checklist (Appendix 1) & Weekly Checklist (Appendix 2) documents.

Any changes required are documented in the Change Management Log.

2.2 Software

All Services and Systems will be monitored on a daily basis and also weekly during the Friday morning maintenance window of 7.00am until 8:30am.

- Downtime – Weekly notification of any unplanned downtime
- Disk capacity maintenance
- Key Applications and Services Active
- Network Availability – Checking of networking switch infrastructure
- VMWare infrastructure updates and Memory and CPU utilisation

Specific Requirements:

- SAN Storage Statistics – Weekly check of the SAN
- Main application system checks
- Other – Webfilter, Firewall, HP Switches, VPN
- All changes documented in Change Management Log

2.3 Patching and Remediation

Patching and vulnerability remediation is key within all systems in use. Patching and remediation should be carried out within the assigned maintenance window where possible. If time constraints do not permit their completion within this time frame, then this work must be rescheduled at a suitable juncture.

Depending on the critical level of the work required, further scheduled downtime to the services and applications affected will be communicated and agreed with the relevant parties to ensure timely resolution.

Where possible, additional patching and remediation work will be addressed at the weekend to reduce the impact of any downtime to online services.

2.4 Windows Updates

Systematic monitoring of all Windows updates and security patches on all servers during the weekly maintenance window. If notified by the computer industry of critical updates, then ICT will determine the course of action depending on the level of impact.

2.5 End-User Devices

Devices use automatic patching where possible. When this is not possible, manual patching will be required.

2.6 Server OS Patching

All servers are patched with the latest updates from Microsoft and other software providers on a weekly basis during the weekly maintenance window. Any updates to the operating system, or to hardware are patched during this period.

Where there is an exigent risk associated with servers and services from an emerging vulnerability, Ark will consider emergency remediation.

2.7 Security Monitoring

Publicly available Internet attached systems and services are subject to a much higher risk than systems located in the internal network. Ark has a system in place whereby the systems are:

- Minimally exposed – using firewalls to ensure only required ports are available;
- Contained – using the DMZ function of the firewall to host our Citrix Netscaler server;
- Protected – using advanced security functions available to the systems or firewalls;
- Tested – regularly assessed for vulnerabilities that may have arisen by automated and manually assured penetration tests.

The use of anti-virus software is managed by our ESET command console, this is used to ensure all ESET agents, modules and software are up to date and to review any threats that ESET highlights.

3.0 Solutions

3.1 Wi-Fi Monitoring

Cloudtrax Wi-Fi Network Monitoring solution is implemented at Head Office. This enables the monitoring and reporting on the corporate Wi-Fi network. All Wi-Fi devices can be monitored for usage and troubleshooting. Within the Services (Ark external offices) Wi-Fi is provided by the on-site routers and Wi-Fi settings and activity are monitored and managed per site.

3.2 Emerging threats

Where a serious vulnerability or emerging threat is discovered, user access is revoked immediately. ICT's only access to the affected servers/services is obtained to quickly address and resolve the problem.

3.3 Penetration Testing

The ICT team arrange for a third party to perform an annual Penetration Test of the external network. If this results in vulnerabilities being found, a plan is drawn up with timescales and responsible owners to action.

Due to the changing nature of vulnerabilities, exploits and the ever-increasing complexity of systems, ICT now utilises a third-party tool, called “IISCrypto” to ensure all external facing services have the latest recommended “Transport Layer Security” (TLS) settings and the “Payment Card Industry Data Security Standards” (PCI) compliant crypto cyphers.

3.4 Web Access Control

Web access is controlled by a dedicated on-site web filtering device. This protects from unwanted website and external services. The device automatically scans for malware and virus-related content. The device has policy driven control that automatically denies access to known inappropriate content and websites.

3.5 Windows Anti-Virus

ESET Anti-Virus Suite is deployed across all Microsoft Windows servers and devices and is maintained using ESET remote administrator console. This console facility enables ICT to manage end point and server security and manages ESET file security on Windows servers and ESET anti-virus software on all other Windows clients.

4.0 Related Documents

Related forms, records or systems used are referenced throughout the procedure.

5.0 Training & Monitoring requirements

5.1 Training

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.

5.2 Monitoring

System monitoring activity is noted throughout this procedure.

Appendix 1 Daily Checklist

1. Check Veeam Backup
2. Check Veeam Replication
3. Check Synology Rsync process & Change Tape
4. Check Eset Security Management Center for Threats
5. Check VMWare Vcenter Appliance Management for Errors
6. Check VMWare Vcenter Vsphere client for errors
7. Check Arkddc1 to check Citrix status
8. Check ICT Help Desk
9. Check Zellis Support Portal
10. Switches/Servers visual healthcheck

Appendix 2 Weekly Checklist

1. Check Eset Security Management Centre for Warnings, File Security updates, Anti-Virus and Remote agent updates.
2. Check All Windows Servers for updates
3. Check All Windows Desktops for updates
4. Check Windows servers for disc space issues
5. Check VMWare Vcenter Appliance Management for Updates
6. Check VMWare Vcenter Vsphere client for host updates
7. Check Xenapp servers for application updates - Firefox/ flash / java etc
8. Check Eset Security Management Center for update to Arkesmc.arkha.org.uk
9. Check Veeam components
10. Update Change Management Log
11. Check DellME5024 SAN Status
12. Clean up Citrix profiles
13. Check PowerEdge R650xs servers for Firmware/Driver Updates
14. Check Dell SAN for Controller and Disc firmware updates
15. Check All HP OfficeConnect 1950 and 1920 switches for firmware upgrades.
16. Check pfSense Netgate firewall for Firmware updates
17. Check pfSense Netgate for Out-of-date rules and configurations
18. Check Veeam for available updates
19. Check for Netscaler firmware updates
20. Check pfSense Netgate for VPN connections