ICT Systems Monitoring & Patching Procedure

Procedure Reference:		G15b	
Related Policy:		G15	
Effective date:	April 2021	**Review date:**	May 2024
Approved by P&PRG:		April 2021	
Owner:	Jean Stevenson	**Job Title:**	Head of ICT
To be issued to:		ARK Management All Staff	
Method of Delivery:		Internal ICT procedure	

Version Control

Date	Owner	Version	Reason for Change
Aril 2021	**Jean Stevenson**	**1.0**	**New supporting procedure to G15**

Summary of Changes

Section	Change

ICT Systems Monitoring and Patching Procedure (G15b)

Contents

1.0 Introduction

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.

2.0 Scope

This Systems Monitoring and Patching Procedure applies to Ark's ICT department and third parties that host or provide ICT services to Ark. The ICT Department, alongside 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. This procedure ensures that all systems are monitored to the necessary level and 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.

3.0 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.

4.0 Requirements

Set out below are the minimal requirements for patching, monitoring and remediation for infrastructure systems. Any production system or service made available to Arks 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.

4.1 Availability and Capacity Monitoring

All Services and Systems will be monitored on a daily basis and also weekly during Friday morning maintenance window of 7am 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

4.2 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 timeously resolution.

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

4.3 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.

4.4 End-User Devices

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

4.5 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.

4.6 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.

5.0 Solutions

5.1 Wi-Fi Monitoring

Cloudtrax Wi-Fi Network Monitoring solution is implemented in the Priory. 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.

5.2 Emerging threats

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

5.3 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 3rd party tool to ensure all external facing services have the latest recommended TLS settings and the PCI compliant crypto cyphers.

5.4 Web Access Control and external Anti-Virus email security

All emails are routed through a third party cloud based email security suite. This external facility includes email spam and anti-virus filtering.

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.

5.5 Windows Anti-Virus

ESET Anti-Virus Suite is deployed across all MS 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.

6.0 Implementation and Review

6.1 Implementation

The Head of ICT is responsible for ensuring that this procedure is followed by ICT staff and relevant third parties.

6.2 Review

The Head of ICT will ensure that this procedure is reviewed at least every three years, and that any amendments required are submitted to the Senior Leadership Team for approval.

7.0 Appendices

7.1 Appendix 1 – Daily Checklist

Check Veeam Backup
Check Veeam Replication
Check Synology Rsync process & Change Tape
Check Eset Security Management Center for Threats
Check VMWare Vcenter Appliance Management for Errors
Check VMWare Vcenter Vsphere client for errors
Check Arkddc1 to check Citrix status
Check ICT Help Desk
Check Zellis Support Portal
Check Capita Portal
Check Daisy Group Portal
Switches/Servers visual healthcheck

7.1 Appendix 2 – Weekly Checklist

Check Eset Security Management Center for Warnings, File Security updates, Anti-Virus and Remote agent updates.
Check All Windows Servers for updates
Check All Windows Desktops for updates
Check Windows servers for disc space issues
Check VMWare Vcenter Appliance Management for Updates
Check VMWare Vcenter Vsphere client for host updates
Check Xenapp servers for application updates - Firefox/ flash / java etc
Check Eset Security Management Center for update to Arkesmc.arkha.org.uk
Run Weekly Process on Capita
Check Veeam components
Update Change Management Log
Bacs Backup to Onedrive Office 365
Copy "IT Share OneDrive" to Onedrive Office 365
Check HP MSA 2050 SAN Status
Clean up citrix profiles
Run "Cleanlogs.PS1" on ARKExch2016
Check Barracuda Time
Check Dell Poweredge R440 servers for Firmware/Driver Updates
Check HP SAN for Controller and Disc firmware updates
Check All HP OfficeConnect 1950 and 1920 switches for firmware upgrades.
Check Zyxel USG-210 for Firmware updates
Check Barracuda WebFilter for firmware Updates
Check USG-210 for Out-of-date rules and configurations
Check Veeam for available updates
Check for Netscaler firmware updates
Check USG for VPN connections