London Ambulance Service NHS
NHS Trust

Patch Management Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document: To establish certain requirements which must be met by all computers connected to London Ambulance Service (LAS) test and live networks

.

Sponsor Department: Information Management and Technology

Author/Reviewer: Information Security Manager. To be reviewed by September 2008

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
	0.1	Information Security Manager	

***Version Control Note:** All documents in development are indicated by minor versions i.e. 0.1; 0.2 etc. The first version of a document to be approved for release is given major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc. until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.

For Approval By:	**Date Approved**	**Version**
Information Governance Group	14/01/08	1.0
Risk compliance and Assurance Group	18/02/08	1.0
Agreed by Trust Board (If appropriate):		

EqIA completed on	**By**
Staffside reviewed on	**By**

Published on:	**Date**	**By**	**Dept**
The Pulse	03/03/08	Records Manager	GDU
LAS Website	12/03/10	Records Manager	GDU
Announced on:	**Date**	**By**	**Dept**
The RIB		Records Manager	GDU

Links to Related documents or references providing additional information		
Ref. No.	**Title**	**Version**

Document Status: This is a controlled record as are the document(s) to which it relates. Whilst all or any part of it may be printed, the electronic version maintained in P&P-File remains the controlled master copy. Any printed copies are not controlled nor substantive.

1. Aim

This Policy establishes certain requirements which must be met by all computers connected to London Ambulance Service (LAS) test and live networks to provide the LAS with a trusted and secure network infrastructure to support the effective delivery of IT resources.

2. Introduction

With our reliance upon IT to conduct our business, the LAS needs to provide an IT service that maintains the operational availability, confidentiality, and integrity of IT systems. Maintaining a set of resources that are patched against known threats and vulnerabilities is core to maintaining an available IT infrastructure. The requirements mandated in this policy attempt to address this.

3. Objectives

1. To create awareness across the Service of the importance of patching all systems pro-actively.

2. To provide a secure network environment for LAS automated applications, staff, business partners and contractors.

3. To provide a resilient set of IT resources that maintains acceptable and agreed levels of confidentiality, integrity and availability.

4. To ensure that all computer devices connected to the LAS network have proper virus-protection software with current virus-definition libraries and the most recent approved operating system and security patches installed.

4. Scope

This policy applies to all computers used on the LAS network that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, staff and third party desktop and laptop computers. Computers that are not physically connected to the LAS network must also abide by this policy. Any exceptions to patch management requirements must be requested in writing (refer to Appendix A).

5. Enforcement

Violations of this policy may result in disciplinary action up to, and including dismissal, and separately, may result in civil or criminal proceedings.

6. Responsibilities

6.1 Information Management &Technology (IM&T) Senior Management Team

- Support the establishment of departmental patch management policy and procedures within the LAS.
- Ensure that funding and personnel are provided to effectively maintain enterprise-wide patch management solutions.

6.2 **IM&T Management Team**

- Ensure that all IT systems are patched in timely manner as laid out in this policy.
- Review current threats and vulnerabilities and to check relevant advisories to monitor any potential threats or vulnerabilities.
- Establish and implement a departmental program for patch management on all IT systems.
- Ensure that all IM&T staff, especially System and Network Administrators are trained and made aware of this policy and relevant procedures.
- Assign system administrators and other authorized personnel specific patch management and vulnerability correction responsibilities.
- Employ the departmental or an approved automated patch management solution to facilitate compliance with this policy and to promote efficiency for all systems, wherever feasible, apply patch management solutions to in-house applications and monitor status of those systems.
- Ensure that a departmental inventory of hardware and software patch status is developed in an electronic database to maintain and track status of all patch actions and vulnerability corrections and to provide rapid response to internal or external reporting requirements.
- Report patch management status monthly to the Information Security Working Group (ISWG) using the Patch Management Compliance Form (see Appendix A).
- Request a formal exception through the established process for any systems which are not compliant within 90 days.

6.3 **Information Security Manager**

- Develop and publish policy and procedural guidance on patch management.
- Provide enterprise-wide tools to assist agencies in compliance efforts.
- Monitor patch management on a department-wide basis.
- Provide advice and guidance to departments in effectively patching systems and eliminating vulnerabilities.
- Support exception requests from the patch management policy to ensure that appropriate security protection is provided.

6.4 **ISWG**

- Members to proactively monitor their own departments IT resources for known threats and vulnerabilities through monitoring advisories and current best practice.
- To review all recommended patching requirements and to classify severity rating of patches in line with the agreed risk matrix (see Appendix B).

- Become familiar with the LAS patch management policy, procedures, enterprise wide solutions and best practice.
- Act as a Point of Contact (POC) for information security to provide guidance and assistance to individuals designated patch management responsibilities.

6.5 **All Staff & Third Parties**

- Must abide by the policy statements set out below
- Must report any suspected lack of compliance with this policy to the ISWG. Failure to do so constitutes a violation of policy.

6.6 **The LAS**

- Reserves the right to monitor for violations of this policy.

7. Policy – general

7.1 Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, approval, installing and verifying.

7.2 Automatic scanning systems, administered from central sites, are superior to manual patching methods and should be employed where possible. It must be possible to define scans by:

7.2.1 IP ranges

7.2.2 Domain/AD groups

7.2.3 Machine Names

7.3 It must be possible to automatically deploy patches from central sites following the same criteria described in 1.2 for scanning.

7.4 If administrative rights to a computer are necessary requirements for a selected automated patch management system, then a local account should be created. Required administrative accounts will follow minimal password standards as laid out in the Password Policy. Default passwords will not be allowed.

7.5 Patch management systems must be able to provide lists of:

7.5.2 Missing Patches and/or Service Packs

7.5.3 Software versions

7.5.4 Patches that were successfully applied

7.5.5 Patches that could not be applied

7.6 The patch management product employed must store all information in a structured database.

7.7 Policy Exception Requirements – IM&T Department Managers will submit all policy exception requests directly to the ISWG. Exceptions to policy will be considered only in terms of implementation timeframes; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature. ISWG will monitor all approved exceptions.

8. Monitoring

8.1 The ISWG and IM&T Management Team will monitor security mailing lists, review vendor notifications and websites and research specific public websites for the release of new patches. Monitoring will include, but not be limited to, the following:

8.2 Scanning the LAS network to identify known vulnerabilities.

8.3 Identifying and communicating known vulnerabilities and/or security breaches to the IM&T Information Security Manager or ISWG members.

8.4 Monitoring CERT, other advisories and websites of all vendors that have hardware or software operating on the LAS network.

8.5 Each IM&T department will create and maintain an organisational hardware and software inventory and an electronic database of information on patches required and deployed on the systems or applications for the purposes of proper internal controls and reporting to the ISWG within constrained timeframes. The ISM reserves the right to review for compliance in patch management and vulnerability correction. This inventory should be centralised where possible and controlled centrally by the IM&T Configuration Manager.

9. Assessing and Classifying Risk

9.1 Once a new patch has been identified, the ISWG will categorise its criticality relevant to each platform (for example, servers, desktops, printers and so on) according to the following:

9.1.1 Emergency -- an imminent threat to the LAS network

9.1.2 Critical -- targets a security vulnerability

9.1.3 Not Critical -- a standard patch release update

9.1.4 Not applicable

9.2 If the ISWG categorises a patch as an Emergency, the group considers it as an imminent threat to the LAS network.

10. Testing

10.1 Once alerted to a new patch, IM&T Information Security will download and review the new patch in line with the period defined within the risk matrix.

10.2 IM&T Customer Services will assess the effect of a patch on the corporate infrastructure prior to its deployment.

10.3 Patches deemed Critical or Not Critical will undergo testing for each affected platform before release for implementation. IM&T Customer Services will expedite testing for critical patches. The department must complete validation against all deployed system images prior to implementation.

10.4 Patches will be tested on non-production systems prior to installation on all production systems.

10.5 Once IM&T CS are satisfied that the deployment of a new patch will not cause any unexpected behaviour, they must agree upon a schedule for deployment.

10.6 It is the responsibility of application owners to identify any problem(s) with a patch(es) and to notify the departmental IT manager of the problem(s). Application and their owners need to be defined and listed in the Configuration Management database.

10.7 It is also the responsibility of application owners to resolve this incompatibility with the application's manufacturer.

10.8 If the manufacturer cannot resolve the incompatibility, the risk incurred by not patching the computer(s) in question must be weighed against the risk of not running the application.

10.8.1 The department IT manager and the application owner should evaluate the options taking into consideration the nature of the vulnerability, the likelihood of its exploitation and the impact to operations of application malfunction.

10.8.2 If they determine that the patch in question should not be deployed, this decision must be communicated to the ISWG.

11. Authorisation and Notification

11.1 The Change Manager must approve the schedule prior to implementation. Regardless of criticality, each patch release requires the creation and approval of a request for technical change (RTC) prior to releasing the patch. The Information Security Manager will decide when notifying staff is necessary.

11.2 IM&T CS will obtain authorisation for implementing Critical patches via an emergency RTC and ISWG approval. The department will implement Not Critical patches during regularly scheduled preventive maintenance. Each patch will have an approved RTC. For new network devices, each platform will follow established hardening procedures to ensure the installation of the most recent patches.

11.3 Since a security patch may cause a system to malfunction, departmental IT managers should proactively announce the deployment of a patch(es).

12. Deployment

12.1 Critical security patches should be deployed within three business days of the time the vendor makes them available.

12.2 Non-critical security and other patches may be applied monthly.

12.3 Relevant IM&T department delegates will deploy Emergency patches within eight hours of availability. As Emergency patches pose an imminent threat to the network, the release may proceed testing.

12.4 Patches that are not deployable with automated patch management solutions will be deployed manually within the timeframes and requirements laid out in this policy.

12.5 In all instances, the department will perform testing (either pre or post-implementation) and document it for auditing and tracking purposes.

13. Verification

13.1 Post-patch audit scans must occur within 1 week after the vendor releases a critical security patch.

13.2 Audit reports must be maintained for at least 1 year.

13.3 IM&T departments, LAN administrators and/or Departmental IT Managers must perform regular or pre-patch network-wide audit scans on all systems and devices at least monthly.

13.4 Following the release of all patches, IM&T Customer Services staff will verify the successful installation of the patch and that there have been no adverse effects.

14. Contingency Planning

14.1 A roaming workstation must have a patch management solution configured to automatically download and install approved patches when it physically connects to the LAS network.

14.2 In the event that a critical patch cannot be centrally deployed, it must be installed in a timely manner either manually or via a vendor maintained update site.

14.3 One or more alternate central console server administrators must be designated and trained so that in the event the primary administrator, Deployment Group or Departmental IT Manager are not available the patch and audit processes can proceed normally.

14.4 Copies of current patches will be maintained by IM&T department delegates and stored in a secure location.

15. Glossary

15.1 **Patches** - typically released to protect against known exploits in operating system or application code or to address functionality issues or a new vulnerability.

15.2 **Vulnerabilities** - weaknesses in software that can be exploited by an entity to gain elevated privileges than it is not authorized to have on a computer or system. Not all vulnerabilities have related patches. These situations require workarounds to attempt to mitigate "unpatched" vulnerabilities.

15.3 **Threats** - A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

IMPLEMENTATION PLAN	
Intended Audience	All LAS Staff
Dissemination	Available to all staff on the Pulse and to the public on the LAS website.
Communications	Revised Policy and Procedure to be announced in the RIB and a link provided to the document.
Training	
Monitoring	Audit reports

Appendix A: Monthly Patch Management Compliance Form

Monthly Patch Management Compliance	
Department_____	***Managers Name***_____
% COMPLIANCE TO APPROVED PATCHES **EMERGENCY** **CRITICAL** **NOT CRITICAL**	**No. OF APPROVED PATCHES NOT DEPLOYED** **EMERGENCY** **CRITICAL** **NOT CRITICAL** **Why?** _____ **Target date for deployment** _____ **Have the vulnerabilities been mitigated through a workaround?** **YES** _____ **NO** _____ ***Please detail workarounds for all patches listed here and attached to this report.***
ISWG Certification Signature: _____ _____ _____ **Name** **Job title** **Date**	

Appendix B: LAS Patch Deployment Matrix

Severity Rating of patches	Impact - PCs or devices affected				
	> 70%	50% - 69%	30% - 49%	11 - 29%	< 10%
Critical					
Important					
Moderate					
Low					

When the vendor releases their patches, these will be looked at based upon the impact to the Service and based upon the quantity of the PCs it affects.

The deployment schedule shown below of vendor patches is based upon the above matrix.

	These patches will be deployed to all PCs affected within 2 - 3 days
	These patches will be deployed to all PCs affected within 1 - 2 weel
	These patches will be deployed to all PCs affected within 2 - 3 weel