London Ambulance Service NHS
NHS Trust

Virus Protection Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document: To ensure effective IT virus detection and prevention

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
12/06/07	0.1	Information Security Manager	First draft

***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**
	LAS Anti-Virus Guidelines	
	Viruses, Malware and Trojans – an introductory listing	
	LAS Internet and Email Acceptable Usage policies	

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. Introduction

This Policy establishes certain requirements which must be met by all computers connected to the London Ambulance Service (LAS) test and live networks to ensure effective virus detection and prevention.

With the evolution of the internet and our reliance today upon connected networks (such as the internet), virus protection is key to maintaining an available IT infrastructure.

Viruses, Trojans and other Malware can spread through the internet at a phenomenal rate. Similarly, a computer connected to the LAS network can spread an infection equally as quickly across our network. Mass infection like this is common and can, at a minimum, inconvenience users. In the worst case scenario, our entire network and all associated services could be unavailable for extended periods of time.

To control this risk, we must ensure the possibility of a virus outbreak is minimised. The requirements mandated in this policy attempt to address this.

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

2. 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, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators.

3. Objectives

1 To create awareness across the Service of anti-virus issues and highlight the importance of protection against these threats.
2 To describe best practice to minimise the risk from viruses and similar Malware.

4. Responsibilities

4.1 **Staff & Third Parties**

- Must abide by the policy statements set out below
- Must be aware of the LAS Virus Protection Policy and Anti-Virus guidelines and review these documents at least every two months for updates.
- Third parties or contractors must seek approval from the Systems Manager or a member of the Systems' Team before using any computer equipment on the LAS network.

4.2 **IM&T Senior Management Team**

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

4.3 **IM&T Management Team**

- Ensure that all IT systems are provided with an anti-virus solution that is managed in line with the statements set out in this policy.

4.4 **Information Security Manager**

- Develop and publish policy and procedural guidance on anti-virus management.

4.5 **The LAS**

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

5.0 Policy

5.1 All LAS PC-based computers must have LAS standard, supported anti-virus software installed and scheduled to run at regular intervals.

5.2 The anti-virus software, detection engine and the virus library files must be kept up-to-date automatically and without user interaction.

5.3 Virus-infected computers must be removed from the network until they are verified as virus-free by IM&T.

5.4 Any activities conducted with the intention to create and/or distribute malicious programs into the LAS networks (e.g., viruses, worms, Trojan horses, email bombs, etc.) are prohibited, in accordance with the LAS Internet and Email Acceptable Usage policies.

5.5 If staff need advice with regard to viruses or suspect malicious activity, please contact the Information Security Manager.

5.6 Any software or information sources (such as floppies, CD's or USB keys) used on the LAS network must be virus scanned before use. This includes information provided by 3rd parties as well as information shared by colleagues or brought from home.

5.7 In a test environment, Lab Administrators are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Refer to the LAS Anti-Virus Guidelines for more guidance.

5.8 To report a suspected virus, please contact the IM&T Service Desk.

5.9 To help prevent virus problems, refer to the LAS Anti-Virus Guidelines, which are available on The Pulse.

6.0 References

Anti -Virus Guidelines
Viruses, Malware and Trojans – an introductory listing (available on The Pulse)

IMPLEMENTATION PLAN	
Intended Audience	LAS Staff and third parties
Dissemination	The Pulse
Communications	Routine Information Bulletin (RIB)
Training	Advise for staff available through the Information Security Manager
Monitoring	Monitoring of system usage