



**London School of Economics
& Political Science
IMTIT Services**

Procedure

Remediating virus outbreaks on public area campus workstations

Jethro Perkins
Information Security Manager

Version	Release 1.2
Date	18 June 2013
Library reference	ISM-PD-100

Table of contents

- 1 Introduction 3**
 - 1.1 Purpose 3
 - 1.2 Scope 3
- 2 Responsibilities..... 4**
- 3 Process 5**
 - 3.1 Problems 5
 - 3.2 Legal and Regulatory Compliance 5
 - 3.3 Compliance with international information security standard ISO27001 5

1 Introduction

Virus outbreaks on campus can have a large effect upon the confidentiality, integrity and availability of information both held by members of the LSE community and centrally within LSE systems. Timely response to any outbreak is critical in order to minimise the damage to user identities of the LSE community, their data and email, and the School's wider reputation. Without a coherent response plan LSE risks becoming the source of the infection of large numbers of its user accounts, puts critical user data at risk of uncontrolled and unapproved alteration and destruction, and risks propagating viruses both within and outside the campus area.

1.1 Purpose

This procedure outlines the responses LSE takes to the infection of any IMT-managed workstation with in a public area of the campus. The aim is to minimise the damage to user data and identities and provide a resolution as quickly as possible.

1.2 Scope

All LSE-built and managed computer systems made available for general use in library and computer rooms on campus and in halls of residence.

2 Responsibilities

IMT Systems Team

Responsible for installation of anti-virus software on LSE-managed computers, and for initiating the re-imaging of infected computers.

IMT Network Team

Responsible for blocking any virus-infected devices from accessing areas of the LSE network.

IMT Student Support

Responsible for the support and replacement of LSE workstations in public areas, as well as any student IT issues.

IMT Information Security Team

Responsible for monitoring and processing reports of virus outbreaks, and for ensuring action is taken to halt any outbreaks, remove any systems providing an ongoing threat and clean any infected systems. Co-ordination with the Janet (Joint Academic Network) Computer Security Incident Response Team.

3 Procedure

Any LSE-managed system in a public area that is the source of a virus outbreak will be blocked from the network as soon as the infection is reported, then physically removed and replaced by the Remote Support Team. This will happen within an hour of Information Security becoming aware that it is the victim of a virus outbreak. This is to reduce as far as possible the number of people infected by using the machine.

The Remote Support Team will keep 3 hot standby machines to ensure the minimum possible service interruption.

The infected machine will be reimaged overnight so that it is ready for a return to service.

3.1 Problems

Any issues with viruses or other malware, including the failure of anti-virus software to update, on machines in public areas should be reported to the IT helpdesk (IT.Helpdesk@lse.ac.uk)

3.2 Legal and Regulatory Compliance

Removing machines from public areas as soon as viruses are discovered helps LSE conform to the following legal regulatory requirements:

Computer Misuse Act 1990 – by acting to reduce scope for unauthorised access to user identities, sessions and data

Data Protection Act 1998 – by acting to reduce scope for unauthorised access to sensitive data

JANET Acceptable Use Policy – by acting to reduce malicious traffic and actions over the network of LSE's internet service provider, JANET

3.3 Compliance with international information security standard ISO27001

The process complies with the following controls of the international information security standard ISO27001:

A.7.1.3 Acceptable use of assets

A.10.1 Operational processes and responsibilities

A.10.4 Protection against malicious and mobile code

A.10.6 Network security management

A.12.1 Security requirements of information systems

A.12.5.4 Information leakage

A.13.2 Management of information security incidents

A.15.1.4 Data protection and privacy of personal information

A.15.1.5 Prevention of misuse of information processing facilities