



London School of Economics & Political Science

IMT

Policy

Hosting Non-Standard Websites and Internet-facing Services

Jethro Perkins

Information Security Manager

Version	Release 1.2
Date	12/12/14
Library reference	ISM-PY-119

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Information Security Policy	3.0	15/03/13	Jethro Perkins
Information Classification Standard	3.0	15/03/13	Jethro Perkins

Version history

Date	Version	Comments
28/10/14	0.1	Initial version
06/11/14	1.0	Release to ISAB
12/12/14	1.1	Incorporating ISAB comments. Release to ITC
	1.2	Incorporating ITC comments.

Review control

Reviewer	Section	Comments	Actions agreed
ISAB	1.2 Example	ISAB felt it would be appropriate to provide more than just one example	Further examples incorporated
ISAB	[General]	Important to explain the method of applying the policy	New section ("1.6 Policy Implementation") created to facilitate this
ISAB	2 Responsibilities	There might be issues beyond information security that need to be considered by the Web Governance Board or its successor when addressing externally-facing websites	Responsibilities section updated accordingly.
ITC	3 Policy	Not all costs will be met by IMT – under some circumstances the cost may have to be met by a project, division or department	Updated accordingly

Table of contents

1	Introduction	4
1.1	Overview.....	4
1.2	Example.....	4
1.3	Aim	5
1.4	Scope	5
1.5	Out of Scope	5
2	Responsibilities.....	6
3	Policy.....	7
3.1	Cost	7
3.2	Demilitarised Zone	7
3.3	Virtual Machine Provision.....	7
3.4	Physical Location and Security	7
3.5	Privileged accounts	7
3.6	Website Governance	7
3.7	Maintaining data security levels	7
3.8	Access Control Authorisation	7
3.9	Operating System Update	7
3.10	Application patching	7
3.11	System Compromise	8
3.12	Support	8
3.13	Service Criticality	8
3.14	Backups.....	8
3.15	Non-compliant services and websites.....	8
3.16	Further Policies, Codes of Practice, Procedures and Guidelines	8
3.17	Review and Development	9

1 Introduction

1.1 Overview

LSE is hosting a number of legacy Internet-facing servers and websites that have traditionally been hosted on physical hardware living in non-datacentre environments, such as people's offices.

As LSE's network is transformed towards a more structured and enterprise-class architecture, it will no longer be possible to continue hosting websites on desktop computers that live outside datacentres that provide appropriate levels of security and environmental control. All computers within LSE will be organised into zones dependent on their function, and at this point, if no provision is made for the transition of these legacy externally-facing servers and websites into a proper Internet-facing zone within an LSE Datacentre, then they will no longer be able to function when the new architecture is in place.

1.2 Examples

"Non-standard websites and Internet-facing services" could include:

- Websites created and maintained by individuals within departments, that sit on a computer on an office desk, and which currently have an 'lse.ac.uk' URL
- Servers that live in offices or LSE comms rooms, are administered part-time by members of a department (who often are employed in teaching or research) and which provide departments or sections within departments with file storage, forums, web servers, email services
- Servers that are used for highly specific computing tasks, and which may be accessible externally by small groups of users, some of whom may not be LSE employees

All these devices are currently running on hardware (they have not been virtualised) and are sitting in LSE's internal network, with ports opened up through LSE's firewall so they can be accessed by the rest of the Internet.

To provide a concrete example, an externally accessible website with a '.lse.ac.uk' address could currently be served from a desktop computer sitting in an office, which is part of LSE's main network (with connections to the Finance and HR systems, file servers etc.) and which has a hole punched through the firewall to it so that the outside world can talk to it. This means that:

- The website has low availability because it is dependent on a single physical machine, which may suffer from mechanical or logical failures, or be subjected to theft or physical damage
- It is less likely to be regularly patched against vulnerabilities, because properly maintaining it is not the primary job of its administrator. Therefore, in addition to the heightened risk it faces because it is externally facing, it is exposed to further risk by a lack of appropriate patching.
- Any websites it provides will not have gone through Web Governance to assess their suitability
- If the machine is compromised, it presents an increased risk to the rest of the LSE internal network, including mission-critical services such as Finance and HR
- It suffers an increased risk of physical compromise, due to being housed in a low-security environment

It is important to make sure that such an Internet-facing service is:

- A suitable part of the LSE brand (if it has an .lse.ac.uk address it is effectively representing the School)
- Highly available, and not dependent on a machine in a single physical location
- Appropriately patched
- Physically secure
- Situated in such a way that it provides the least risk to LSE mission-critical services

It should therefore be hosted on a highly available virtual machine within LSE's secure datacentres, and be placed within a "Demilitarised Zone" (DMZ) where, unlike in the current model, its access to more sensitive LSE services (such as Finance and HR) will be blocked. If it hosts a website, the site should be assessed by the Web Governance Board before being made and only re-enabled if the board feel it is an appropriate part of the LSE web estate.

The architecture outlined in the solution above is the method being used with all current projects involving externally-facing resources.

1.3 Aim

This policy aims to provide consistent provision for externally-facing servers and websites that have so far fallen outside LSE's governance procedures and which are currently hosted in such a manner that they will become unavailable when a more secure network architecture is implemented. It aims to balance increased security for mission-critical resources with the need to provide a platform for members of the School to fulfil their teaching and research requirements.

1.4 Scope

1. Internet-facing servers and websites currently run on hardware not in LSE's two Datacentres and which are not administered by IMT.
2. Future provision for Internet-facing servers and websites hosted by LSE and administered by non-IMT personnel.

1.5 Out of Scope

Centrally-provided Internet-facing services e.g. LSE website, staff and student 'personal' web pages. STICERD servers.

1.6 Policy implementation

Due to resource restrictions, there will be no 'big bang' approach to policy implementation. Help to migrate internet-facing services to suitable platforms will be provided as issues arise. A comprehensive migration package will be implemented as part of any rollout of network zoning across LSE.

2 Responsibilities

System Owners

The owners of Internet-facing servers and websites are required to ensure:

- Any applications, scripting languages etc are kept up to date
- Data made available to external access is either appropriate for global consumption or else is restricted with suitable access controls
- The servers or websites do not host or accept any type of payment card data
- Reports of vulnerability or compromise (whether from IMT, Janet CSIRT, UK-CERT, US-CERT or any other incident response team) are dealt with immediately.
 - This includes the withdrawal of the Internet-facing service until such time that the vulnerability or compromise has been eliminated
- Submitting any proposed or existing website to the Web Governance Board (or its successor) for approval.
- Security of any account credentials

Web Governance Board (or successor)

Ensuring any website that falls in the lse.ac.uk address space is an appropriate externally-facing LSE resource. This will involve ethical, aesthetic and public relations considerations, as well as any information security concerns.

Department of Information Management and Technology:

Systems Team

- Provide VM or hosting space upon a VM for Internet-facing systems, applications and websites.
- Host VM across secure Datacentre locations.
- Ensure physical security of host systems.
- Patch host system and VM Operating Systems.
- Provide SSH Gateway access.

Network Team

Provision of DMZ

Academic Support Teams

Provision of any help required by the end user

Information Security Manager:

- Co-ordination of incident response.
- Authorisation for blocking/takedown of any LSE services, systems or websites that are compromised, transmitting malware or otherwise endangering LSE's mission critical services and the security of its data.
- This policy and its updates.

Information Security Advisory Board

Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

Information Technology Committee

Responsible for approving information security policies.

3 Policy

3.1 Cost

The cost of providing the virtual machines will in many cases depend on the size and complexity of the requirement. Some costs for basic service provision will be met by IMT, whereas the costs of larger or more complex services would be expected to be met by the project, department or division requiring the service.

3.2 Demilitarised Zone

All Internet-facing LSE resources must sit in a DMZ. This provides additional protection to LSE's internal network (including mission critical services such as HR and Finance) in the event that the Internet-facing resource is compromised.

3.3 Virtual Machine Provision

The Internet-facing resource will be provided with either a VM or space on a VM in order to run the service. Services will not run on physical hardware ("baremetal").

3.4 Physical Location and Security

The VM hosts will be located in LSE's secure Datacentres.

3.5 Privileged accounts

Privileged accounts will be provided where there is an appropriate requirement for them. It is the responsibility of the account user to keep the account credentials secure.

3.6 Website Governance

All websites transferred to this service will be reviewed by the Web Governance Board before they are made externally available.

3.7 Maintaining data security levels

It is the responsibility of the site or service owner to ensure that data is appropriately secured.

3.8 Access Control Authorisation

Access will only be provided for explicitly named system owners who are current LSE employees. If a person ceases being an LSE employee access will be revoked.

3.9 Operating System Update

Patching the Operating System (OS) will be performed by IMT. The OS will be patched even if it breaks any applications: it is the responsibility of the application owner/developer to ensure applications function with the OS

3.10 Application patching

As stated in 3.8, it is the responsibility for the application owner/developer to patch the application and to ensure any security updates to scripting languages, application platforms etc. are performed within a month of the patch release.

3.11 System Compromise

Any system, application or website that is reported compromised, whether by a member of IMT, Janet CSIRT, UK-CERT or other security incident reporting body, must be investigated by the owner immediately. Any externally-facing service reported compromised will have external access removed while the investigation and any remedial measures take place.

A system or service proved compromised must be returned to a vanilla state.

3.12 Support

Help and support will come from the Academic Support teams.

3.13 Service Criticality

Anything provided as part of this service will not be defined as mission critical

3.14 Backups

Backups will not be provided by default. It is the responsibility of the service owner to ensure backups are taken.

3.15 Non-compliant services and websites

Any Internet-facing services and websites falling under the remit of this policy that are not migrated to the provided service will not function once LSE's new network architecture is implemented.

3.16 Further Policies, Codes of Practice, Procedures and Guidelines

This policy sits beneath LSE's overarching [Information Security Policy](#). Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on LSE's website. All staff, students and any third parties authorised to access LSE's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

The below list of current policies is in no way authoritative and new policies will be published on the LSE website as they become available.

Associated policies:

[Information Security Policy](#)
[Conditions of Use of IT Facilities at LSE](#)
[Policy on the use of mobile telephony equipment](#)
[Policy on the use of school-funded iPhones](#)
[Conditions of use of the residences network](#)
[Password Policy](#)
[Asset Management Policy](#)
[Data Protection Policy](#)

Procedures:

Account Procedures

Standards and Guidelines:

[Information Classification Standard](#)
[Encryption Guidelines](#)
[Remote and Mobile Working Guidelines](#)
[Guidelines on the use of Cloud storage](#)

3.17 Review and Development

This policy shall be reviewed and updated regularly by the Information Security Advisory Board (ISAB) and an auditor external to IMT as appropriate to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.