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 acces 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 polices:

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.