Security Standards and Procedures

Security Management in Practice

Policies, standards, procedures and guidelines

- What are the differences between these?

Policies, standards, procedures and guidelines

Policy – high level statement of an organisation's values, goals and objectives in a specific area, and the general approach to achieving them.

E.g., Information Security Policy

Policies, standards, procedures and guidelines

Standard – more prescriptive than policy, states what needs to be done and provides consistency in controls that can be measured.

E.g., The ISF Standard of Good Practice for Information Security

Policies, standards, procedures and guidelines

Procedure – set of detailed working instructions that will describe what, when, how and by whom something should be done

E.g., Handling Copyright Infringements Notification Procedure

Policies, standards, procedures and guidelines

Guidelines – not obligatory buy can provide advice, direction and best practice in instances where it is difficult to regulate how something should be done (e.g., out of office working).

E.g., Guidelines for using Dropbox and other cloud storage providers

Security Management in Practice

Policies, standards, procedures and guidelines

- Documentation needs to be clearly written and precise.
- Where possible, statements should contain positive rather than negative ‘do not’ cases – promote the correct way rather than the wrong way of doing things.
- Need to be endorsed by senior management, and have clear ownership (e.g. HR, manager).

Organisational Security Policy

How will the enterprise manage information assurance?

The protection of information assets in accordance with their criticality

The compliance with legal and regulatory obligations

The means by which **users will be made aware of information assurance issues** and the **process to deal with breaches to policy** and suspected assurance weaknesses

The fact that this policy has the support of the board and chief executive

Organisational Security Policy

Useful resources for developing organisational security policy:

- ISO/IEC 27000 series
- Information Security Forum (ISF) Standard of good practice https://www.securityforum.org/tool/the-standard-of-good-practice-for-information-security/

Organisational Security Policy

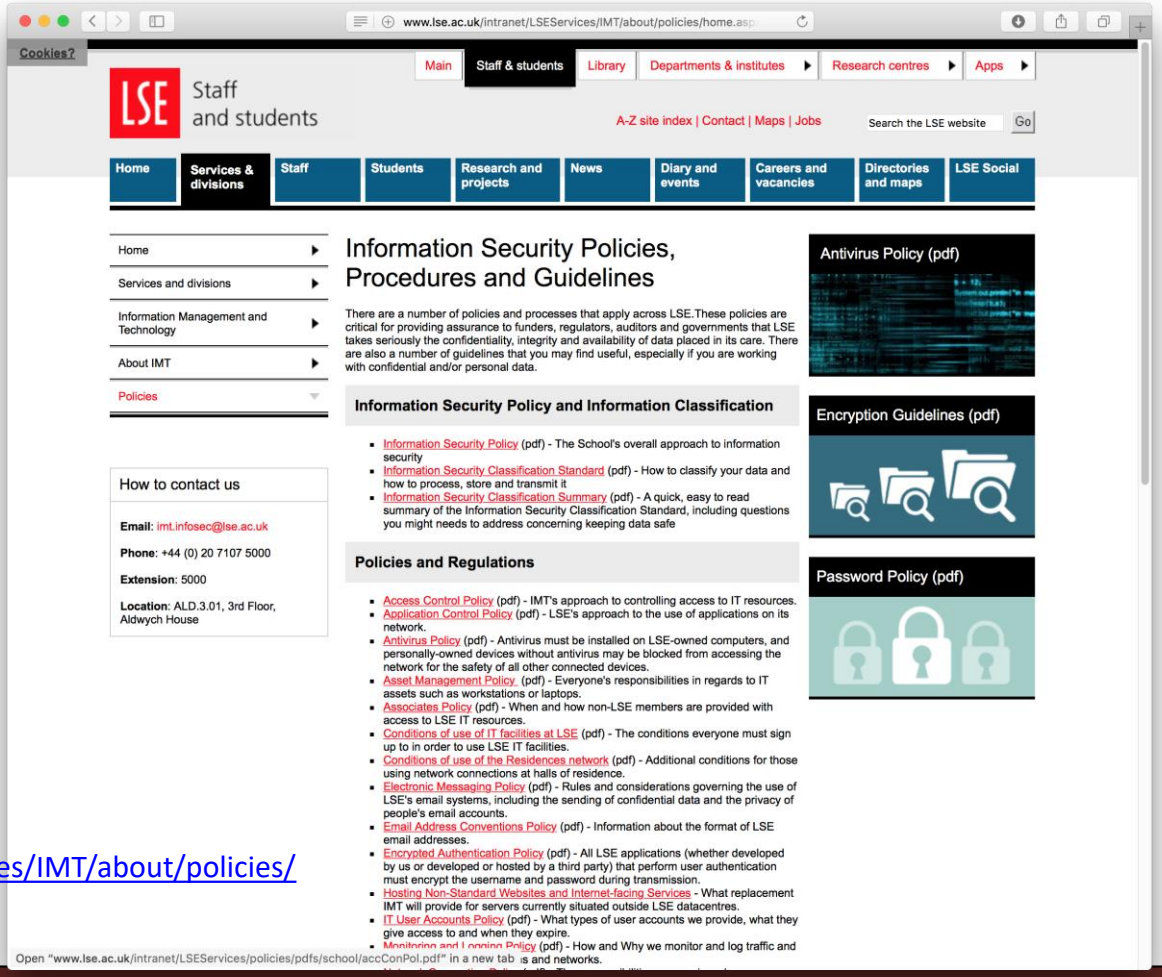
Useful resources for developing organisational security policy:

- COBIT (Control Objectives for Information and Related Technology) – another framework for IT management and IT governance, produced by ISACA. http://www.isaca.org/cobit/pages/default.aspx

- SANS Top 20 Critical Security Controls. https://www.sans.org/critical-security-controls/vendor-solutions/

Examples of Policies, Procedures and Guidelines

LSE provide a clear set of policies, procedures and guidelines online



- http://www.lse.ac.uk/intranet/LSEServices/IMT/about/policies/home.aspx

Review, evaluation and revision of security policy

- Reviews should take place after any significant changes to either systems or resources, or as part of a regular review schedule.

- Review schedule should indicate all persons involved and a formal record of any revisions made, with explanation of when content is either added or removed.

Review, evaluation and revision of security policy

Review should consider:

- Changes to technology, processes, organisation, resource availability or working practices
- Changes to contractual, regulatory or legal requirements
- Changes in threats and vulnerabilities
- Results, actions and recommendations from any assurance reviews or audits
- Findings and recommendations from either incidents or previous assurance breaches, or when there is non-compliance with the policy

Security Audits and Review

- Audits and Reviews provide a good opportunity to understand how well things are working with the enterprise.
- Typically will be performed by an impartial third party. Access rights during review should be restricted on a need-to-know basis, with a monitor log to trail activities.
- Non-Disclosure Agreements (NDAs) may be required if review involves sensitive information.
- Formal report of the review is produced that specifies corrective action if necessary, and timescales for implementing these.

Checks for compliance with security policy

- Compliance checks help to identify whether controls are still adequate and relavent. Also gauges level of user understanding and awareness of assurance responsibilities.
- If non-compliance is found, this could be due to lack of training, misunderstanding or a disregard of processes.
- Action taken should reflect the level of non-comformity – is it a one-off incident or a wider problem?
- Results are reported to management and fed into future policy reviews

Security incident reporting, recording and management

All people in the organisation need to know how to recognise an incident and who to report it to.

5 phases of incident management:
reporting, investigation, assessment, corrective action, review.

Incident report includes who they are, where they are, contact details, brief description of incident, any danger to life health or company assets, any actions taken so far, and time of incident.

From first report to close, a log should be kept of information, decisions made, and consequences of actions that can be used later (internally and externally).

Incident response teams and procedures

- Cross-sectional team from organisation that deal with incident response.

- Liase with law enforcement and national bodies (if deemed appropriate):
  - Computer Emergency Response Team (CERT) UK
    - GovCertUK, MODCert
  - National Crime Agency (NCA)
    - National Cyber Crime Unit (NCCU)
  - Centre for Protection of National Infrastructure (CPNI)

Recap

- Policy. Standards, Procedure and Guidelines
- Review, evaluation and revision
- Compliance
- Security Incident Reporting