1. Introduction

1.1. The University relies on computer systems and, to a lesser extent, manual procedures for handling and processing the information supporting many of its activities. Information that the University manages shall be appropriately secured to protect against consequences of breaches of confidentiality, failures of integrity, interruption to availability and failure to comply with legal requirements. (The University must comply with relevant statutory or other overriding requirements affecting information security, whether or not they are explicitly stated within its policies.)

1.2. This is the top-level document, in a hierarchically structured set of documents, specifying information security policy for the University of Leicester (hereafter referred to as the University). This document includes:

- The purpose, scope, and structure of the security policy documentation.
- Responsibility for information security policy documentation.
- Developing and maintaining the policy document set.
- Implementing information security policies.
- Responsibilities for implementing information security policies.
- References to related documents.

2. Purpose of University information security policy documentation

2.1. Maintaining effective University information security policy documentation provides a sound basis for regulating how systems and procedures are designed, configured and operated. Regulation is necessary to ensure that information is adequately secured against adverse affects on availability, integrity, confidentiality or compliance.

2.2. University policy documentation should perform these functions:

- Present a comprehensive and coherent approach to information security at a strategic level.
- Reflect the intentions of the University e.g. by defining expected standards.
- Facilitate on-going development, scrutiny and revision of policies at strategic and tactical levels.
- Provide guidance or direction to users, administrators and developers of University information systems.
- Describe an ideal model, against which reality can be compared, to identify areas where policy is not being implemented well and policies that need to be revised.

3. Scope

3.1. The policies in this documentation set apply to all information systems:
- Owned by the University.
- Being used for University business.
- Connected to networks managed by the University.

3.2. The policies in this documentation set apply to all information:
- The University is handling whether or not it is owned by the University.
- Including software owned or licensed by the University.

3.3. The policies in this documentation set apply to all people:
- Managing or using any system identified in 3.1 above.
- Responsible to the University and handling information identified in 3.2 above.

4. Structure of the policy documentation set

4.1. The structure and content of this policy documentation set is based on an approach set out in the "UCISA Information Security Toolkit". The Toolkit is intended to help academic institutions to formulate and maintain policy documents, and is based on the control guidelines contained in the industry standard framework BS7799 (ISO27001).

4.2. This top-level document references a set of policy sub-documents all of which have equal standing, which state official University policy in various areas. These policy sub-documents will be referred to as "Strategic Policy" documents.

4.3. Each strategic policy document should only contain high-level descriptions of expectations and principles: they are to be deliberately free from practical details of policy implementation and regulations.

4.4. Where necessary, details expanding on how statements in the strategic policy documents are to be implemented should be described in "Policy Implementation" documents. These policy implementation documents are below the strategic policy documents in the documentation hierarchy.

4.5. Explicit regulations, typically in the form of simple dos and don'ts, shall be derived from either strategy or implementation level documents. These regulations will be grouped together in "University Regulations" documents according to whom they apply, rather than according to the area of information security they relate to. (These documents sit below the implementation documents in the hierarchy). This approach is intended to facilitate "delivery" of all relevant regulations to the correct target audience in a succinct form.

4.6. Statements in strategic, implementation and regulation documents must fully reference each other. This must be done to ensure that:
- Any available implementation details or regulations related to a strategic policy statement can easily be found.
- The strategic context of all implementation details can be identified.
- The implementation details (if there are any) and strategic context of every regulation can be traced.
4.7. Diagram summarising the policy documentation system structure:

![Diagram](image)

5. Responsibility for information security policy documentation

5.1. The Information Communications Technology Committee (ICTC) has ultimate responsibility for approving updates and additions to the University information security policy documentation set. (This process will distinguish current official University policy documents from any other legacy or unofficial accounts of policy).

5.2. The policy documentation set will be reviewed at least annually; however, urgent requests for updates will be processed as quickly as possible.

5.3. Proposed changes and additions to the policy documentation may be submitted by any member of staff, via a Head of Department, ultimately for consideration by the ICTC.

5.4. Proposed updates to policy must be fully converted into proposed changes to the policy documentation. This must be done in such a way that implications for all related documents are fully taken into account. An update will only be considered approved when each resulting new or modified document has been approved.

6. Developing and maintaining the policy document set

6.1. The policy document set must be maintained as a whole to keep it internally self-consistent and also to maintain a uniform style.

6.2. Duplicated content and ambiguity should be removed.

6.3. The documentation set should be extended and revised over time to ensure that it remains comprehensive and current.

6.4. The documentation should be kept free from superfluous detail to make it easy to read and maintain.

6.5. To facilitate managing the documentation, the status, version history and approval history must be maintained for each document.

6.6. Document updates pending approval must be easily distinguishable e.g. by using different colour text.
7. Implementing information security policies

7.1. Measures will be taken by the University to implement information security policies including:

- Establishing a continuous "Plan-Do-Check-Act" cycle of activities which ensure that suitable practices are documented, reinforced and improved with time. (Documentary evidence of the processes and procedures involved will be required to demonstrate implementation of policy to external parties.)

- Ensuring that all individuals who use information systems, or otherwise handle information, understand the policies that are relevant to them and any consequences for non-compliance. **In cases of policy violation deemed to be serious, wilful or repeated the University will not hesitate to take disciplinary action.**

- Using physical security measures where deemed necessary.

- Applying technology where considered appropriate and feasible. For example, to control and log access to systems, data and functionality.

- Using various lawful forms of monitoring activities, data and network traffic to detect policy infringements.

- Taking into account relevant information security policy requirements when planning and undertaking activities involving IT-based information systems.

- Formal or informal risk assessment, to identify the probability and impact that various hazards could have on information systems.

- Monitoring effectiveness of its information security policy implementation. This may involve review independent from those charged with its implementation.

8. Responsibilities for implementing information security policies

8.1. It is the responsibility of the University to sufficiently resource and direct implementation of its information security policies.

8.2. Responsibility for applying University information security policy to Departmental or Divisional information systems is delegated by the University to the Heads of Department or Division respectively. Heads are responsible for any further delegation of functions relating to policy enforcement.

8.3. Individuals must understand and agree to abide by University policies before being authorised for access to any information systems for which the University has responsibility.
9. References to strategic level policy sub-documents

<table>
<thead>
<tr>
<th>Name</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Asset Protection Policy</td>
<td>ISP-S2</td>
</tr>
<tr>
<td>Compliance Policy</td>
<td>ISP-S3</td>
</tr>
<tr>
<td>Outsourcing and Third Party Access Policy</td>
<td>ISP-S4</td>
</tr>
<tr>
<td>Personnel Policy</td>
<td>ISP-S5</td>
</tr>
<tr>
<td>Operations Policy for IT Service Providers</td>
<td>ISP-S6</td>
</tr>
<tr>
<td>Information Handling Policy</td>
<td>ISP-S7</td>
</tr>
<tr>
<td>User Management Policy</td>
<td>ISP-S8</td>
</tr>
<tr>
<td>Use of Computers Policy</td>
<td>ISP-S9</td>
</tr>
<tr>
<td>System Planning Policy</td>
<td>ISP-S10</td>
</tr>
<tr>
<td>System Management Policy</td>
<td>ISP-S11</td>
</tr>
<tr>
<td>Network Management Policy</td>
<td>ISP-S12</td>
</tr>
<tr>
<td>Software Management Policy</td>
<td>ISP-S13</td>
</tr>
<tr>
<td>Mobile Computing Policy</td>
<td>ISP-S14</td>
</tr>
<tr>
<td>Teleworking Policy</td>
<td>ISP-S15</td>
</tr>
<tr>
<td>Cryptography Policy</td>
<td>ISP-S16</td>
</tr>
<tr>
<td>ResNet Acceptable Use Policy</td>
<td>ISP-S17</td>
</tr>
</tbody>
</table>

Failure to comply with University Policy may lead to disciplinary action.

Document history:

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 March 2007</td>
<td>(C. Nelson)</td>
<td>Began first draft.</td>
</tr>
<tr>
<td>24 May 2007</td>
<td>(C. Nelson)</td>
<td>Table of policy sub-documents added.</td>
</tr>
<tr>
<td>5 June 2007</td>
<td></td>
<td>Approved.</td>
</tr>
<tr>
<td>16 August 2010</td>
<td>(C. Nelson)</td>
<td>ISP-S2 is renamed “Information Asset Protection Policy”.</td>
</tr>
<tr>
<td>18 May 2011</td>
<td>(C. Nelson)</td>
<td>Revisions resulting from review within IT Services.</td>
</tr>
</tbody>
</table>

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.