1. Introduction

1.1. This information security policy document contains high-level descriptions of expectations and principles relating to operation of University information systems. This is a sub-document of Information Security Policy (ISP-S1).

1.2. This document includes statements on:

- Physical security
- Insurance
- Critical information assets
- Operational procedures, controls and responsibilities
- Reporting Information Security Incidents
- Reporting Software Faults

2. Physical security

2.1. Physical threats to information security include:

- Environmental threats - temperature, humidity, fires, floods, storms
- Supply system threats - disruption to energy supply, communications
- Manmade threats - unauthorised access, tampering, theft, wilful damage, accidents

2.2. The physical security of University information systems must be managed appropriately, taking into account their importance to the business operations of the University and the types and quantities of information they hold.

2.3. Physical security arrangements must be considered when new information systems are being planned and arrangements must be reviewed if circumstances change.

2.4. An assessment of the physical threats and vulnerabilities affecting important information systems must be undertaken. Where necessary specialist advice should be obtained to support this assessment. The cost of possible countermeasures to physical security threats must be taken into consideration. Countermeasures should be implemented where deemed appropriate, effective and justified.

2.5. Taking into account any countermeasures to be implemented, a decision must be made by management about how to handle any physical risks that may remain. The options are: consider further countermeasures, accept the residual risk or transfer the risk.

2.6. See also:

- Managing Information Asset Security (ISP-I4)
2.7. New building security measures and changes to existing measures must be agreed and operated with collaboration between the department responsible for the information system and Estates (Estates and Facilities Management Division).

2.8. When building or maintenance work is to take place, the risks that the work may present to any information systems must be assessed and managed. Risks must be managed with collaboration between the department responsible for the information system and Estates.

2.9. See also:
   - Building Security (ISP-I1)

3. Insurance

3.1. The risk of loss or destruction of University owned computers or data should be offset by appropriate levels of insurance cover. *(Clearly whilst this can help to offset the cost of replacing lost computer hardware, it will not help to recover lost information that has not been backed up securely elsewhere.)*

3.2. The University property insurance policy does not cover laptops and smartphones. *(In particular, note that University smartphones managed by IT Services are not supplied with any insurance cover.)*

3.3. Estates Insurance Services Office offer advice about insurance and can arrange specific insurance for items not covered by the University property insurance policy. For example cover for University mobile computing hardware, including laptops and smartphones, can be arranged.

3.4. To activate cover for other computer and peripheral devices that are not taken offsite, such as desktop PCs and printers, departments must ensure that the items are on the departmental insurance schedule. The schedule is to be revised and returned to Estates Insurance Services Office annually.

3.5. Estates Insurance Services Office must also be specifically notified of each additional high value item or where there are significant changes in computing hardware. A web form for doing this is available on the University Insurance Website:
   - [http://www.le.ac.uk/estates/customercare&_office_support/insurance/computer/index.html](http://www.le.ac.uk/estates/customercare&_office_support/insurance/computer/index.html)

4. Critical information assets

4.1. At the departmental level, University Governance and Planning requires development of business continuity plans covering business processes defined as “critical”. Departmental information assets, such as computers or information stores, which need to be replaced or restored to service within 72 hours of failing or becoming unavailable, would be considered to represent a “critical risk”. Inclusion of these in the departmental business continuity plan is required. For further information refer to the University of Leicester business continuity planning procedures (contact University Governance and Planning).

5. Operational procedures, controls and responsibilities

5.1. The procedures for the operation and administration of the University’s key information systems must be documented, and those procedures and documents regularly reviewed and maintained.

5.2. Staff involved in administering, developing, testing and commissioning systems, must follow appropriate change management procedures.
5.3. When reviewing key systems and procedures, explicit consideration should be given
 to whether segregating duties and areas of responsibility would help to reduce the risk of
 information security incidents and be feasible.

6. Reporting Information Security Incidents

6.1. Procedures will be established and widely communicated for reporting security
 incidents and suspected security weaknesses in the University’s business operations and
 information processing systems. Mechanisms shall be in place to monitor and learn from
 those incidents.

6.2. See policy sub-document:

   - Reporting Information Security Incidents (ISP-I3)

7. Reporting Software Faults

7.1. Procedures will be established for reporting software malfunctions and faults in the
 University’s information processing systems. Faults and malfunctions shall be logged and
 monitored and timely corrective action taken.

7.2. See policy sub-document:

   - Reporting Software Faults (ISP-I2)

---

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

---

Document history:

<table>
<thead>
<tr>
<th>Date</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 March</td>
<td>Began first draft.</td>
</tr>
<tr>
<td>3 July</td>
<td>Minor change.</td>
</tr>
<tr>
<td>16 July</td>
<td>Title changed as agreed by the Steering Committee and a minor addition suggested by Prof. Hillman.</td>
</tr>
<tr>
<td>24 July</td>
<td>Revised in consultation with Graham Middleton.</td>
</tr>
<tr>
<td>06 July</td>
<td>As advised by the Steering Group, removed “for which it is necessary to accept some residual risk” from “It is recommended that key systems, for which it is necessary to accept some residual risk, are given consideration in a business continuity plan.”</td>
</tr>
<tr>
<td>16 August</td>
<td>ISP-I4 is renamed “Managing Information Asset Security”.</td>
</tr>
<tr>
<td>25 August</td>
<td>Some improvements and additions.</td>
</tr>
<tr>
<td>Date</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>22 September 2010 (C. Nelson)</td>
<td>Liz Gordon recommended stressing that University mobile phones provided through IT Services are not automatically insured.</td>
</tr>
<tr>
<td>13 October 2010 (C. Nelson)</td>
<td>Incorporated changes to the section about insurance as recommended by David Masters.</td>
</tr>
<tr>
<td>02 November 2010 (C. Nelson)</td>
<td>Approved by the Steering Group.</td>
</tr>
<tr>
<td>18 May 2011 (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.