1. Introduction

1.1. This document supports implementation of “operational level protection of information assets” as referred to in Information Asset Protection Policy (ISP-S2) and “physical security” as referred to in Operations Policy for IT Service Providers (ISP-S6).

1.2. The term “information asset” is used below to refer to a useful or valuable:
   - Store of information in any format
   - Information processing system of any type
   - Facility used to transfer information

1.3. An approach to conducting a basic information security assessment is outlined below. This is offered as guidance for departments or individuals wishing to ensure that many risks, that commonly affect information assets, are systematically reviewed. (Additional guidance in this area is offered by Information Assurance Services.)

2. Operational protection of information assets and strategic risk management

2.1. It is important to note that the procedure outlined here is not an alternative or replacement for the University’s mandatory strategic risk management policy, which requires each department to establish and maintain its own strategic risk register. The procedure described here supports that strategic risk management process by working at a lower level, helping to identify and assess risks to departmental information assets. Regardless of what leads to significant risks to the business of the department being identified, such risks must be reported to senior management for potential inclusion in the departmental strategic risk register.

3. Methodologies

3.1. Various methodologies can be applied to assessing the risks to information assets. Some approaches are more quantitative whilst others are mainly qualitative. Whilst deploying a good quantitative risk assessment methodology has potential to give the most objective and repeatable results, quantitative methods are rarely used to measure risk in information assets. Reasons for this include difficulty of determining sufficiently accurate input data and poor cost-effectiveness. (Quantitative approaches often revolve around use of specialised software applications.) A simple qualitative approach, based on judgement, best practice and experience, is a practical proposition capable of producing useful results.

4. Risk optimisation

Broad systematic consideration of information security risks with prioritised defensive action is more likely to be cost-effective than implementing measures piecemeal. It is rarely feasible and often not desirable to attempt to reduce risks to zero. This is because there is normally a point at which marginal risk reduction ceases to be cost-effective or would unacceptably hamper a business activity. Availability of resources and "risk appetite" are major factors in determining security levels. Risk management is intended to
tie these factors together by assisting management in determining where to direct resources to achieve acceptable risk levels at an acceptable cost.

5. Requirements

5.1. Information security assessment may be undertaken by an individual or a team. However, the team approach is recommended because a broad range of knowledge may be required and group discussions help when weighing up perceived risks. (For convenience the text below will refer only to using a team.)

5.2. The information security assessment team should have access to extensive knowledge of both the departmental information assets to be examined and understanding of the significance of those assets to the business activities of the department and University.

5.3. Senior management approval, support and input is required if security of departmental information assets is to be managed effectively. The assessment team may require special authorisation from management to examine systems and processes in detail. Senior management will also need to review significant findings and make decisions about implementing any challenging or costly security measures.

6. Selecting and scoping information assets for review

6.1. The locally managed information assets of most importance to the business activities of the department should normally be prioritised for review. If the assessment team is charged with deciding which assets to focus on then it must first be clear on the context in which it is working. What is important to an individual or small group may not be as important in the wider context.

6.2. It is necessary to judge an appropriate level of granularity at which to work so as not to generate too much or too little detail. It may be possible to group similar assets together so that they can be assessed and treated collectively. In some cases it may be more practical to assess an information system or business activity in its entirety rather than analysing each of its components separately. IT and non-IT asset examples:

- An IT asset that delivers a particular business function may include locations, power supply, networking, servers, data storage, client PCs, users and administrators.

- A paper-based information asset may be a processing system involving handling and processing paperwork in several locations, movement of paperwork between locations and the personnel involved.

6.3. The team should ensure there is good common understanding of what each asset does and includes. Details about each asset to be considered should include:

- Purpose and what it includes
- Where it is located
- What information it handles
- Whether it is used to store personal data about living people
- Dependence on any other departmentally managed assets or facilities
- Dependence on any assets or facilities managed outside the department
- How long it could be unavailable before the situation would become unacceptable
7. Identifying potential risk areas

7.1. A methodical way to identify areas of possible concern is to consider a checklist of threat types in relation to each information asset being assessed. Any areas which may require further consideration should be noted. For a list of common threat types that may impact information assets see:

- Information Asset Security Measures (ISP-I8)

8. Assessing risk levels

8.1. Assessing levels of risks to information assets will almost certainly involve making judgements based on imperfect information. For most scenarios statistical likelihood data will be limited or unavailable and potential impact may also be difficult to estimate. However, identifying significant concerns is of more practical importance than attempting to assign precise risk level values.

8.2. Review and give more detailed consideration to the assets and the applicable threat types that have been noted. If, on further consideration, a specific and relevant risk can be defined, then assess its risk level. Refer to the risk level matrix and descriptions in Appendix 1.

9. Reporting, logging and managing information asset risks

9.1. Risks that have been assessed should be recorded and reported through line management.

9.2. The status of risks should be reviewed regularly by management to decide which of these possible actions is currently appropriate:

- Accept - the risk is to be accepted because it’s worth taking or is unavoidable
- Reduce - measures to help reduce threat likelihood or impact are to be taken
- Transfer – responsibility for bearing or mitigating the risk is to be transferred to another individual or organisation
- Escalate - it is an unacceptable risk that must be escalated because it cannot be managed locally

9.3. Risk ownership should be assigned to an individual or group who realistically can be expected to manage the risk and who could take action deemed necessary for adequate mitigation of the risk. Risks that cannot be managed by the current risk owner should be escalated.

9.4. Proposals for risk mitigation measures are to be considered by management, who will consider factors including whether proposals are affordable and justified.

9.5. Where mitigating actions are to be taken, priorities and timescales should also be decided. In addition to a list of threat types, some generic suggestions for mitigation are included in:

- Information Asset Security Measures (ISP-I8)

9.6. Senior management should add risks of strategic significance to the departmental risk register for ongoing management and monitoring.
Appendix 1

Risk level matrix:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Rare</th>
<th>Unlikely</th>
<th>Possible</th>
<th>Likely</th>
<th>Almost Certain</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>4</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>C</td>
</tr>
<tr>
<td>3</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>2</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>1</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
</tbody>
</table>

Risk level descriptions:

Low (L)  This risk can be tolerated, as the necessary mitigating action is already taken on a routine basis, through established local management processes.

Medium (M)  This risk can still be tolerated, but some additional mitigating action will need to be implemented, beyond that already taken on a routine basis, and monitored by local managers.

High (H)  This risk can only be tolerated if significantly increased and/or additional mitigating action is implemented and closely monitored by senior management.

Critical (C)  This risk cannot be tolerated. A detailed and comprehensive action plan will need to be implemented as a matter of urgency, and closely monitored, with the aim of reducing this risk to a lower level.

---

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

---

Document history:

15 August 2007  (C. Nelson)  Began first draft.

27 September 2007  (C. Nelson)  Began reworking the procedure.
<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 March</td>
<td>2008</td>
<td>(C. Nelson) Now outlines an approach instead of including the specifics of the procedure to be used.</td>
</tr>
<tr>
<td>26 February</td>
<td>2009</td>
<td>(C. Nelson) Minor changes.</td>
</tr>
<tr>
<td>3 July</td>
<td>2009</td>
<td>(C. Nelson) Minor change.</td>
</tr>
<tr>
<td>13 July</td>
<td>2009</td>
<td>(C. Nelson) Added likelihood timescale to table 1.</td>
</tr>
<tr>
<td>18 August</td>
<td>2009</td>
<td>(C. Nelson) Reviewed and approved by Phil Simpkin.</td>
</tr>
<tr>
<td>19 August</td>
<td>2010</td>
<td>(C. Nelson) ISP-S2 is renamed “Information Asset Protection Policy” ISP-I4 is renamed “Managing Information Asset Security”. Reworked, including harmonising the choice of risk likelihood and impact descriptions with those to be used in departmental risk registers (as specified by the University Governance and Planning section).</td>
</tr>
<tr>
<td>08 October</td>
<td>2010</td>
<td>(C. Nelson) Approved, with minor changes, by Neil Cox. Approved by Phil Simpkin.</td>
</tr>
<tr>
<td>02 November</td>
<td>2010</td>
<td>(C. Nelson) Approved by the Steering Group.</td>
</tr>
<tr>
<td>18 May</td>
<td>2011</td>
<td>(C. Nelson) 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.