1. Introduction

1.1. This information security policy document describes expectations and principles for protecting the security of University information assets. This is a sub-document of Information Security Policy (ISP-S1).

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. This document includes statements on:
   - University strategic risk management and business continuity planning
   - Departmental business continuity plans
   - Departmental local strategic risk registers
   - Operational level protection of information assets

2. University strategic risk management and business continuity planning

2.1. The University seeks to exercise effective control against the possibility that a specific event or set of circumstances will adversely affect the achievement of its strategic objectives in the medium and longer term. Implementing controls appropriately to protect security of the information assets, on which University business processes depend, is consistent with this aim. See also:
   - University of Leicester Risk Management Policy

2.2. The University has developed procedures for strategic risk management and business continuity planning that must be implemented across the University. Implementation of this strategic departmental risk management and business continuity planning is the responsibility of departmental and divisional heads. The overall project is administered by the Governance Section within the Division of Student and Academic Services.

2.3. These strategic risk management and business continuity planning processes have an important role to play in supporting information security, as outlined in the next two sections.

3. Departmental business continuity plans

3.1. At the departmental level, the University’s procedures require development of business continuity plans covering processes defined as “critical”.

3.2. 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.

3.3. For further information refer to the University of Leicester business continuity planning procedures (contact the Governance Section).

4. **Departmental local strategic risk registers**

4.1. At the departmental level, the University requires local strategic risk registers to be established.

4.2. It is appropriate that significant information security risks, such as risks to important information assets, should be given visibility and monitored using this risk register.

4.3. Departmental local strategic risk registers should be maintained in accordance with the University of Leicester strategic risk management procedures (contact the Governance Section).

5. **Operational level protection of information assets**

5.1. Departmental senior management will generally be aware of any strategic level risks affecting the locally managed information assets on which their business processes depend. Where these risks are significant they will be recorded in the departmental risk register and monitored. Where an information asset represents a critical risk, it will also be featured in the departmental business continuity plan.

5.2. At the day-to-day level, operational managers and other staff must take an active role in identifying risks to University information assets within their areas and in protecting them where that can reasonably be expected.

5.3. This operational level protection of information assets should involve:

   - Recognition and assessment of risks, including new risks
   - Acceptance or assignment of responsibility for managing risks where practical
   - Upward reporting of significant risks which are not, or cannot, be managed
   - Upward reporting of new strategic risks, whether or not they are being managed
   - Undertaking, where appropriate, suitable prevention or remediation measures

5.4. Protecting information assets against damage or disruption must be undertaken with due consideration of:

   - The value and importance of the asset
   - The types and levels of risks to which the asset is exposed
   - The likely effectiveness of any protection measures
   - The cost of protection measures

5.5. A simple systematic approach can be helpful in assessing how well an IT or non-IT based information asset is protected from a range of common threats. Should such an approach be used and result in the identification of any significant risks to the work of the department, then those risks must be reported for potential inclusion in the departmental risk register. Information Assurance Services offers to provide further details about how to use the approach that is outlined in this document:

   - **Managing Information Asset Security (ISP-I4)**
Document history:

3 July 2009  (C. Nelson)  Minor changes.
13 July 2009  (C. Nelson)  Updated the information about business continuity.
18 August 2009  (C. Nelson)  Reviewed and approved by Phil Simpkin, also minor changes made as suggested.
16 August 2010  (C. Nelson)  ISP-I4 is renamed “Managing Information Asset Security”.
08 October 2010  (C. Nelson)  Approved, with minor changes, by Neil Cox. Approved by Phil Simpkin.
02 November 2010  (C. Nelson)  Approved by the Steering Group.
18 May 2011  (C. Nelson)  Revisions resulting from review within IT Services.

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.