1. Introduction

1.1. This document gives additional details about implementing the "Reporting Information Security Incidents" policy stated in Operations Policy for IT Service Providers (ISP-S6).

2. Rationale for centralised reporting of information security issues

2.1. It is important that information security incidents, and suspected information security weaknesses, are reported, logged, then dealt with.

2.2. Information security issues should be reported to IT Services, because IT Services:

- Is responsible for many key University information systems and must be made aware of any potential threat to those systems
- Is the division of the University Administration that specialises in providing IT services and support
- Has overall responsibility for ensuring that University networks connected to JANET are not misused. Most computer equipment used by the University is connected to these networks
- Is empowered to prohibit devices suspected of being compromised, misused or misconfigured, from connection to University networks until the issue is resolved
- Provides services enabling the University to fulfil its statutory obligations in relation to the Data Protection Act
- Will discretely handle any information security issues that are reported

2.3. The result of reporting an issue to IT Services should be that:

- Necessary resources are allocated to investigating and monitoring the issue until it has been resolved. *(The profile of issues logged may inform IT Services’ development decisions.)*
- Where necessary and feasible, measures to counter problems will be implemented as quickly as possible
- Other organisations are advised or consulted about incidents as appropriate, and in particular:
  - Security incidents involving the loss of sensitive or confidential information are to be reported to the Estates Insurance Services Office (x7630 or email insurance@le.ac.uk) and Information Assurance Services (x7946 or informationsecurity@le.ac.uk) as soon as possible
  - Incidents such as fire, flood or theft affecting IT systems are to be reported promptly to both the Estates Security Office (emergencies x888, other calls x2023 or email control@le.ac.uk) and the Estates Insurance Services Office (x7630 or email insurance@le.ac.uk)
Where the cost of recompiling lost data may become the subject of an insurance claim, the Estates Insurance Services Office (x7630 or email insurance@le.ac.uk) is to be informed promptly.

- The relevant Directors of College and Heads of Department are informed by IT Services of the incident where this is appropriate.

3. Reporting information security incidents

3.1. Staff and students must report to IT Services, information security incidents and any suspected security weaknesses found in relation to any University IT-based information systems. This applies to all systems that are used for University business or connected to University networks, whether or not they are administered by IT Services.

3.2. Information system security incidents (suspected or confirmed) relating to University of Leicester computers, data, networks or people should normally be reported to the IT Service Desk (x2253 or ithelp@le.ac.uk). Where the matter to be reported is sensitive or urgent it may be reported to Information Assurance Services (x7946 or informationsecurity@le.ac.uk).

3.3. The details of security issues must be properly logged by IT Services (i.e. who, what where and when). Logs should include a description of the issue, history of actions taken and status of the problem on closure.

3.4. Breaches of security, where serious Staff or student misconduct is suspected, will be reported to the Registrar and Secretary who will decide any further action to be taken.

4. Reporting other types of security incident

4.1. Security incidents not relating to IT, involving suspected or actual breach of University physical security, possible crime, possible theft or violence must be reported to the Estates Security Office (Security Lodge):

- The Estates Security Office is distinct from Information Assurance Services.
- The University Estates Security Office is located in the Security Lodge, Wyggeston Drive, University Entrance No 1.
- Where appropriate the Estates Security Office will contact IT Services regarding any security matters relating to University information systems.
- To contact the Estates Security Office in emergencies the internal phone extension number to call is 888, for other enquiries call extension 2023.
- Where appropriate the Estates Security Office will contact Estates Insurance Services Office Services (using the 24hr contact number as necessary)

---

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

---

**Document history:**

23 March 2007 (C. Nelson) Began first draft.

3 July 2009 (C. Nelson) Minor change.
Title changed and instructions on reporting physical incidents to Estates Security Office added as agreed by the Steering Group.

Revised in consultation with Graham Middleton.

Simplified section 2.3. IT Services will advise or consult other organisations about incidents as necessary or appropriate (which includes the Estates Security Office). Further clarification about reporting other security incidents.

The Estates Insurance Services Office must be informed promptly of: loss of personal data, loss of data for which cost of replacement may become the subject of an insurance claim and fire or flood incidents affecting IT systems.

Some minor changes made as approved by the Steering Group.

Revisions resulting from review within IT Services.

Requirement of ITS to inform Head of Department where appropriate.

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.