



UNIVERSITY OF LEEDS

Terms of Reference Information Security Group

Version 3.1
8 March 2011

© University of Leeds 2011

The intellectual property contained within this publication is the property of the University of Leeds.

This publication (including its text and illustrations) is protected by copyright. Any unauthorised projection, editing, copying, reselling, rental or distribution of the whole or part of this publication in whatever form (including electronic and magnetic forms) is prohibited. [Any breach of this prohibition may render you liable to both civil proceedings and criminal penalties].

Document Control

Owner:	Kevin Darley, IT Security Co-ordinator, Information Systems Services, University of Leeds
Source Location:	V:\document\isms\ISG Terms of Reference ISG.doc
Document Reference:	
Other Documents Referenced:	
Related Documents:	Information Security Policy Supporting Policies
Acknowledgements:	

This document is subject to change control and any amendments will be recorded below.

Change History

Version	Date	Circulation	Changes
1.0	28/05/04	http://campus.leeds.ac.uk/isms	First formal issue
2.0	18/09/08	http://campus.leeds.ac.uk/isms	
3.0	12/10/10	ISG	Dates and membership
3.1	8/03/11	http://www.leeds.ac.uk/informationsecurity	Changes agreed and published

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available at <http://www.leeds.ac.uk/informationsecurity>. Those to whom this Policy applies are responsible for familiarising themselves periodically with the latest version and for complying with Policy requirements at all times.

1. Introduction

1.1. Background

The University of Leeds is in the process of developing an Information Security Management System (ISMS) in accordance with the principles of ISO 27001 (formerly ISO17799 [BS 7799]), the Code of Practice for Information Security Management. The purpose of the framework is to deliver policy and controls through which members of the University are able to use the IT/IS infrastructure in a manner that will:

- protect key data and information from security breach so that it remains accurate and available;
- provide controls which enable sensitive information to be kept confidential; and
- protect both individuals and the University from inadvertent breach of information related legislation.

In 2003 the University published its Information Security Policy which provides a high level commitment by the University to adhere to the best principles and practices of information security. The Policy is now formally owned by the Vice-Chancellor's Executive Committee (VCEG) having been signed-off by Senate after review and acceptance by the Committee on Information Strategy, Systems and Services (CISSS), ADC and the Planning & Resources Committee (PRC), all of which have since been dissolved. The Policy can be found at <http://www.leeds.ac.uk/informationsecurity/>.

The Information Security Policy is a framework which is being augmented through the introduction of Supporting Policies. These supporting policies focus on specific areas of information security, for example mobile and remote access to University information, and in some cases on specific audiences, for example members of staff who support computer systems and services. The supporting policies are being developed through consultation with members of the community, and are to be approved and managed by the Information Security Group (ISG) which is empowered to do so by VCEG, in accordance with the Information Security Policy.

2. Structure & Role

2.1. Membership

The ISG comprises the following full-time members:

- Head of Information Technology (Chair) – Philip Hobley (ISS);
- University IT Security Co-ordinator – Kevin Darley (ISS);
- Two senior members of the academic community:
 - Subhajit Basu (School of Law)
 - VACANT;
- Two senior members of the corporate community:
 - David Wardle (Head of Corporate Services)
 - Linda Mortimer-Pine (Deputy Director of Human Resources);
- A Faculty IT Manager – John Dodds (MaPS);
- The Chair of the Network Special Interests Group (NetSIG) – David Waller.

In addition, periodically it may be necessary for additional members to be co-opted on an ad-hoc basis when particular specialist knowledge is required (e.g. legal issues).

If the group considers it appropriate particular reports will be made available to other committees and individuals (for example the Head of the Security Service)

Membership of the group will be reviewed periodically and changes may be made to the membership subject to the effectiveness of the group.

2.2. Scope & Responsibilities

The purpose of the ISG is to:

- Ensure that proposed Policy is both comprehensive and comprehensible;
- formally approve the adoption of supporting policies on behalf of VCEG;
- consider requests to change a supporting policy and to approve or reject these as appropriate;
- ensure appropriate institutional or local consultation is undertaken before agreement, or changes, to the Information Security Policy or Supporting Policies;
- consider requests to issue policy exemption certificates and to approve or reject these as appropriate;
- review major incidents - and any other events that have serious information security implications - and the proposed measures to prevent recurrence;
- review 'information-related' risk assessment findings and recommended controls;
- review information security audit findings and recommendations;
- oversee the development of the University's information security strategy;
- update VCEG on information security framework development and progress and serious Policy transgressions.

2.3. Method of Working

The ISG is to work using e-mail exchange whenever possible. However the group will meet every three months.

Meeting dates, times and venues are to be scheduled in advance to minimise the risk of members being unable to attend.

The remit of this group makes it inappropriate for deputies to be sent should a member be unavailable to attend a meeting.

In the event of several members of the group giving notification that they are unable to attend a scheduled meeting, the meeting may be re-scheduled.