Loughborough University

Information Security

Introduction to Information Security

Approved
June 2016

www.lboro.ac.uk

Introduction to Information Security

Introduction

The University's Information Governance Policy notes the key role which information plays across the full range of the work of the University. Staff, students and some external partners need to access information and the University's information systems to carry out their daily activities. The University also provides a range of information for the public. The University recognizes the need for an appropriate balance between openness and confidentiality in the management and use of information. To achieve this aim and ensure the University complies with its legal responsibilities, a suite of information security policies has been developed to guide staff, students and external partners on how to use and handle University information whilst maintaining a level of confidentiality appropriate to the nature of the information. The policies are also relevant to members of the public who may wish to access information about the University.

Purpose and Key Definitions

This policy provides an introduction to the University's Information Security Policy Framework and includes links to all policies in the Framework.

By **Information** we mean any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphical, cartographical, narrative, or audiovisual.

By **Information Security** we mean the management of information to allow appropriate access and use for those who need it whilst preventing unauthorized access which might result in a breach of the University's legal responsibilities, the rights of individuals or might present a reputational risk to the institution. It includes arrangements to reduce the risk of copying, modification or deletion of information where this is not legitimate for the conduct of University activities.

The term "**the University**" in the Policy Framework should be interpreted in the widest sense and includes relevant activities, services and systems related to all Schools and Professional Services of the University as well as related to IT Services.

The risks to maintain good information security may be deliberate or accidental human acts, or arise from technical or environmental factors.

Confidentiality - Confidentiality is the need to ensure that information is disclosed only to those who are authorised to view it.

Information Systems – Any system, service or infrastructure used to process information or the physical locations housing them. This includes critical business environments, business processes, business applications (including those under development), computer systems and networks.

Personal Data – Any data held in a system, whether electronic or hard copy, that identifies a living individual (for a legal definition, see the Data Protection Policy

www.lboro.ac.uk/admin/ar/policy/dpact/ludpp).

UCISA – Universities and Colleges Information Systems Association

www.ucisa.ac.uk/

Scope

This policy provides a framework for the management of information security throughout the University and applies to:

- All those with access to University information and information systems, including staff, students, partners and contractors;
- Any systems attached to the University IT or telephone networks and any systems supplied by the University;
- All information stored or processed by the University for its operational activities, regardless of whether it is stored or processed electronically or in hard copy form, including any communications sent to or from the University and any University information held on systems external to the University network;
- All external and third parties that provide services to the University in respect of information processing facilities and business activities.

Aims

The Information Governance Policy sets out the following principles for Information Security:

- The University will establish and maintain policies for the effective and secure management of its information.
- The University will undertake or commission regular and appropriate assessments and audits of its information and IT security arrangements.
- The University will promote effective confidentiality and security practice to all its staff, students, partners and suppliers through policies, procedures and training as appropriate.
- The University, through the Information Governance Sub-Committee of the Information Technology and Governance Committee will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and information security.

The University is committed to protecting the security of its information and information systems in order to ensure that:

- The integrity of information is maintained, so that it is accurate, up to date and 'fit for purpose';
- Information is always available to those who have a legitimate need for it and there is no disruption to the business of the University;
- Confidentiality is not breached, so that information is accessed only by those authorised to do so;

- The University meets its legal requirements, including those applicable to personal data under the Data Protection Act;
- The reputation of the University is safeguarded.

The policy framework structure is based on the "UCISA Information Security Toolkit" which, in turn, is based around the ISO 27000 series standards. It provides guidance on the Information Categories and Controls for different types of information (Public, Not Sensitive, Confidential, and Confidential) and a series of policies aimed at both general (e.g. All Staff and Research Students) and more technical audiences (e.g. IT Operations Policy).

The University is committed to providing training to ensure staff, students and partners understand the importance of information security and, in particular, exercise appropriate care when handling Confidential and Highly Confidential information. It also provides specialist advice when required.

Responsibilities

The Information Governance Policy sets out the responsibilities of key University bodies and senior staff in relation to Information Security. The responsibilities of all staff and research students and of taught students are set out in the relevant policies below.

Training and specialist advice on information security is available from Academic Registry and IT Services (M.Lister@lboro.ac.uk).

IT Governance Committee and Information Governance Sub-Committee

The Information Technology and Governance Committee (ITGC)

http://www.lboro.ac.uk/committees/it/

with support from the Information Governance Sub-Committee (IGSC), is responsible for:

- Ensuring that users are aware of this policy;
- Seeking adequate resources for its implementation;
- Monitoring compliance;
- Conducting regular reviews of the policy, having regard to any relevant changes in legislation, organisational policies and contractual obligations;
- Ensuring there is clear direction and visible management support for security initiatives.

Information Security Policy Framework

The Information Security Policy Framework sits under the overall Information Governance Policy and is made up of the following sub-policies:

- Introduction to Information Security (this policy) (relevant to all)
- Information Categories and Controls Policy (relevant to all)
- Responsibilities of All Staff and Research Students
- Responsibilities of Taught Students (Acceptable Use Policy)
- Information Services and Service Contractors Policy (relevant largely to IT professionals or others involved in procuring IT related services)

- Information Sharing Policy (relevant to all)
- Mobile Working Policy (relevant to all)
- Policy on the Management of User Access to Information (relevant to all)
- IT Operations Policy (relevant to IT professionals)
- Information Security Incident Handling and Review Policy (relevant to all)

The following policies are also relevant to all staff and students (taught and research):

- Data Protection Policy
- Freedom of Information Policy
- Copyright Policy
- Software Policy