



**London School of Economics
& Political Science
IT Services**

**Standard
Information Security Classification**

Stephan Freeman
Information Security Manager

Summary	This document lays out the different levels of security classification for electronic and physical documents within LSE. This will be superseded by a formal document ratified by the Information Security Group once it has been formally established.
Version	1.0
Date	16 July 2010
Library reference	ISM-SD-007

Document control

Distribution list

Name	Title	Department
Adrian Ellison	Assistant Director, Infrastructure Services	IT Services
Amber Miro	Assistant Director, User Services	IT Services
Andy Coulthard	Assistant Director, Management Information Systems	IT Services
Rachael Maguire	Records Manager	Planning and Corporate Policy Division
Kevin Haynes	Senior Assistant Secretary	Planning and Corporate Policy Division
Stephan Freeman	Information Security Manager	Technical Infrastructure Group, IT Services
James Hargrave	User Support Manager	User Support, IT Services
Tim Green	IT Manager	Library
Nic Warner	Computer Manager	STICERD
Sue Donnelly	Archivist	Library

External document references

Title	Version	Date	Author

Version history

Date	Version	Comments

Review control

Reviewer	Section	Comments	Actions agreed

Table of contents

1	Introduction	4
1.1	Purpose	4
1.2	Scope	4
1.3	Background	4
1.4	Assumptions	4
1.5	Conventions	4
1.5.1	<i>Font styles</i>	4
1.5.2	<i>Bullets</i>	5
1.5.3	<i>Notes, warnings, tips and suggestions</i>	5
1.5.4	<i>Tables</i>	5
2	Responsibilities.....	6
3	Security Information Classification	7
3.1	Overview of policy:	7
3.1.1	<i>Public</i>	7
3.1.2	<i>Internal use</i>	7
3.1.3	<i>Confidential</i>	7
3.1.4	<i>Secret</i>	7
3.2	Overview of classifications	8
3.3	Delegation of roles and responsibilities	8
3.3.1	<i>Explicit</i>	8
3.3.2	<i>Written</i>	8
3.3.3	<i>Specific to an individual or role</i>	8
3.4	Granularity of classification	8
Appendix A	Sign off form	9

1 Introduction

1.1 Purpose

LSE holds many significant information assets that must be protected against unauthorized access, disclosure or modification, or other misuse. Different types of information require different security measures, making proper classification of information assets critical to effective enterprise security. LSE's information classification policy is designed to provide information owners with guidance as to how to classify information assets properly.

This guidance — developed in accordance with the LSE's Information Security and Record's Management Policies — includes classification criteria and categories, as well as rules for the delegation of classification tasks.

1.2 Scope

This document covers the levels of security classification for information and limited recommendations for its protection.

It does not attempt to classify any particular information nor does it have any bearing on the legal requirements for document retention or record classification.

This document must be read in conjunction with the Records Management Policy and Information Security Policy.

1.3 Background

LSE handles many different types of information. As part of the development of both the Records Management Policy and Information Security Policy, a need was identified that a standard for classifying the sensitivity of information was required to go with a set of recommendations on how to store this information.

Individual creators, owners or handlers of LSE information must apply this classification system to their information.

1.4 Assumptions

The mechanisms offered as recommendations in this proposal exist and are available to those that need them.

The reader has sufficient technical knowledge to implement the controls set out in this standard.

1.5 Conventions

A number of different styles of text and page layout are used within this document. This section describes the use of these styles together with examples.

1.5.1 Font styles

Bold is used to emphasise important information.

Italic is used for file and directory names, URLs and registry key names. Italic is also used to indicate a filename or comments within a code section. Italic is also used for the first reference to a vendor or product where doing so improves clarity.

`Constant width` is used to indicate sections of code and program names.

Constant width with italic is used to indicate parts of code to be replaced depending on certain conditions.

Constant width with bold is used to indicate text typed by the user in code sections.

1.5.2 Bullets

Bullets appear indented in relation to the paragraph indentation with a nested bullet available in a different style:

- Bullet
 - Nested bullet

1.5.3 Notes, warnings, tips and suggestions

Notes, warnings, tips and suggestions are

These boxes hold important details relevant to the surrounding text

1.5.4 Tables

Tables appear as follows:

Header Row (Repeated on each page if the table splits across a page)
Data Row

2 Responsibilities

Information Owners are responsible for assessing information and classifying its sensitivity. They should then apply the appropriate controls to protect that information.

IT Services should provide the mechanisms to protect electronic information while it is resident on an LSE-controlled system. IT Servers should also provide advice and guidance on the use of any systems it provides for end users to use.

All LSE staff and students must respect the security classification of any information and, if any information is found with a security classification, in an inappropriate place, they must report this to the Head of Security or Information Security Manager as soon as possible.

3 Security Information Classification

3.1 Overview of policy:

Information owners must assign one of the following four classifications (see Table 1) to any information assets under their control:

3.1.1 Public

Public information (for example, programme and course information on LSE's website, or the LSE Experts' Directory) can be disclosed or disseminated without any restrictions on content, audience or time of publication. However, the disclosure or dissemination of the information must not violate any applicable laws or regulations — such as privacy rules — and modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the computer system.

3.1.2 Internal use

Internal use information can be disclosed or disseminated to appropriate members of LSE, partners and other individuals, as appropriate by information owners without any restrictions on content or time of publication.

3.1.3 Confidential

Confidential information is subject to access restrictions of some type. These restrictions may apply to all or part of the content, to the intended audience for the information, or to the time of publication. All access to confidential information requires that the users first successfully authenticate themselves to the computer system. Disclosure or dissemination of this information is not intended, but it would not result in severe damage to LSE.

3.1.4 Secret

Secret information has significant value for LSE, and unauthorized disclosure or dissemination would result in severe damage to LSE. All information that is not explicitly classified as public, internal use or confidential is to be considered secret. Access to secret information must be controlled by strong authentication — user ID and password are not sufficient — and is permitted only for specific named individuals. All access attempts must be logged. Storage and transmission of secret information must be protected by encryption.

Designating information as secret involves significant costs to LSE. For this reason, information owners making classification decisions must balance the damage that could result from unauthorized access to or disclosure of the information against the cost of additional hardware, software or services required to protect it.

The default level for unclassified data is *Internal Use*.

3.2 Overview of classifications

Classification	Examples of Information	Typical Amount	Security Costs	Examples of Security Measures
Public	Programme and course information on LSE's website	Many documents	Negligible	Write-protected file format
Internal Use	Company policies and procedures	Many documents	Low	Windows and Unix directory access Kept in a drawer
Confidential	Project or personal documents, individual student records, exam scripts	Majority of documents	Medium	Windows and Unix file access Kept in a locked drawer or safe
Secret	Large amounts of HR systems, LSE Central data, research data	Selected documents	Very high	Secure access token, card reader, and intrusion detection or intrusion prevention tools Kept in a safe

Source: Gartner (November 2006)

3.3 Delegation of roles and responsibilities

By default, information is owned by the person or role that created or obtained it. However, departments may delegate ownership, and information owners may delegate ownership further, defining ownership on a more detailed level. However, such delegation must be:

3.3.1 Explicit

The default information owner must specifically identify the affected information assets (for example, room, folder or database) and notify the new information owner of the change. The current owner must identify respective information resources and must notify the new owner of the change. Implicit delegation (for example, by job description) is not acceptable.

3.3.2 Written

Verbal delegation of information ownership is not acceptable.

3.3.3 Specific to an individual or role

Information ownership must be delegated to a specific person or to a role with which a specific person can be identified. Ownership cannot be delegated to a group.

Note: Information ownership can involve significant costs. For this reason, the delegation of ownership should be accompanied by the assignment of budgetary responsibility.

3.4 Granularity of classification

The sets of information being classified should, in general, be large rather than small. Smaller units require more administrative effort, involve more decisions and add to complexity, thus decreasing the overall security.

Appendix A Sign off form

Library reference: ISM-SD-007

Information Security Classification

Assistant Director, Technical Infrastructure Group: Adrian Ellison

Signed: Date:.....

Comments:

Assistant Director, User Services: Amber Miro

Signed: Date:.....

Comments:

Assistant Director, Management Information Services: Andy Coulthard

Signed: Date:.....

Comments:

Records Manager: Rachael Maguire

Signed: Date:.....

Comments:

Senior Assistant Secretary: Kevin Haynes

Signed: Date:.....

Comments:

Information Security Manager: Stephan Freeman

Signed: Date:.....

Comments:

Archivist: Sue Donnelly

Signed: Date:.....

Comments: