UNIVERSITY OF
BIRMINGHAM

SOFTWARE LICENSING POLICY

Version 12/12/2012

David Deighton, IT Services

CONTENTS

1. Policy on Software Licensing

1.1 Software Licensing Compliance

1.1.1 The scope of this Policy on Software Licensing applies to the following:

i. University staff (rather than students)
ii. Software on workstations (e.g. PCs, MACs and laptops) as well as servers.
iii. Software on workstations in either of the following categories:
   a. Workstations which belong to the University.
   b. Workstations which are privately owned, but which are being used for University business and supported by the University.

1.1.2 The University has a responsibility to ensure that all software used by members of the University using hardware supplied or supported by the University, is appropriately licensed.

1.1.3 Individual users of software applications have a responsibility to ensure that:

i. software installed on workstations for which they have some responsibility is licensed.
ii. the software is either named on the list of University/College list of approved and supported software, or otherwise use of the software has been agreed with/notified to the College IT Manager (or equivalent manager for Corporate Services).
iii. the software is not named on the list of prohibited software maintained at the University/College (or Corporate Services) level.
iv. they are complying with the conditions of use of that licence.

1.1.4 A central list of supported software approved for use within the University will be maintained by IT Services and College IT Managers, as well as a list of specifically prohibited software (e.g. on security grounds or inappropriate use of University resources). Use of software which may not require a licence, e.g. Freeware or Shareware, may only be used if it is on the list of officially approved software. Usage of approved screensavers will be specified at the College level.

1.1.5 Each user must take responsibility (in conjunction with the authoriser and installer) for their own particular use of software, in accordance with the licence terms and End User Licence Agreement.

1.1.6 The University's Conditions of Use of Computing and Network Facilities (Section 3) contains the following stipulations concerning use of licensed software – failure to comply with these could constitute a disciplinary offence:

i. The University reserves the right for access to be granted to computer audit staff without notice to enable them to check against an inventory of licensed software and hardware. Any unlicensed software or hardware or illicit copies of documentation will be removed by such audit staff and reported to the Director of IT Services, who may initiate disciplinary proceedings."
ii. Where software has been electronically downloaded from IT Services computer systems requiring user authentication by means of a username and password, the user must read and comply with the licensing conditions for that software, and the act of

downloading indicates acceptance of the licensing conditions pertinent to that software.

iii. All persons who are licensed to use software or who control access to any computing and/or network resources are obliged to take all reasonable care to prevent the illicit copying and use of software and documentation.

iv. No one shall introduce on to computer systems any software or other material requiring a licence for which a valid licence is not in place.

1.2 SOFTWARE INVENTORIES

1.2.1 A software inventory must be set up and centrally maintained at the College level, with responsibility for this taken by the College IT Manager, and similarly a nominated IT Services manager being responsible for the software inventory within Corporate Services. The format should be as close as possible to the University standard format specified by IT Services.

1.2.2 This software inventory will be used to match the number of software licenses purchased against the number of staff licences in use; also to check that the software licences are current, i.e. have not expired. This monitoring must be carried out on a regular basis, and licences purchased appropriately if required to rectify any discrepancies identified.

1.2.3 The inventory must take account of staff leavers, i.e. identifying software licences that are no longer being used. Unused software licences remain the responsibility of the College IT Manager. Any transfer of such licences between Colleges should be recorded within the inventory.

1.2.4 The same managers responsible for the software inventory are also responsible for maintaining copies of the software licences relating to the inventory.

1.2.5 Use of Freeware/Shareware software should also be monitored in order to ascertain firstly that use of the software is actually free for use for business use within the University, and secondly that the use of such Freeware/Shareware does not pose any security risks. Beyond carrying out these checks, it is not necessary to either record the usage of such software, or maintain copies of software licences.

1.3 SOFTWARE PURCHASING

13.1 Software purchasing must be limited just to IT staff, together with any other nominated individuals authorised by the College IT Manager. A list of such additional authorised individuals must be documented and maintained by the College IT Manager.

1.3.2 These authorised members of staff must also sign off individual software purchases.

1.4 STORAGE OF SOFTWARE MEDIA AND LICENCES

1.4.1 Software and media must be stored in a suitably secure and accessible location, and take into account the Business Continuity requirements, including for the case of loss of a server, or even potential loss of a building.

1.4.2 The location of the software media should be recorded on the software inventory.

1.4.3 Similar consideration must be given to software which has been electronically downloaded, and it should be stored on an appropriate server. A hard copy of the licence or certificate should also be stored.

1.5 AUTHORISED INSTALLATION OF SOFTWARE

1.5.1 Only authorised IT Staff within IT Services or College IT support staff are permitted to undertake installation of software. Other non-IT staff will be permitted to undertake installation of software only if authorised on the exception list maintained by the College IT Manager (or equivalent).

1.5.2 The same IT installation staff (or other staff specifically authorised to install software) are also responsible for ensuring that the software which they are installing is appropriately licensed and recorded in the relevant software inventory.

1.6 SOFTWARE AUDIT AND USE OF AUDIT TOOLS

1.6.1 Wherever possible, access to the use of software by individuals should be controlled by Active Directory, thereby enabling both potentially automatic distribution of software applications, as well as automated use of audit tools

1.6.2 Support staff, either in IT services centrally, or within Colleges, have the responsibility for using these automated audit tools to ensure compliance by the University, i.e. confirmation that the number of licences held corresponds with the actual number of users of the software as specified by the licence conditions.

1.6.3 An exception list of those devices which are excluded from such an audit must be specified at the College level, e.g. laptops and devices on the wireless network.

1.6.4 All University workstations and servers must have the standard corporate tools installed on them as part of their build to enable the software monitoring to take place. Any exception to this must be authorised and documented at the College level.

1.6.5 If suitable automated tracking software is available, support staff should use this in order to identify any software which may no longer be required within the University, with a view to either re-utilising such software, or arranging for its disposal if redundant.

1.7 DISPOSAL OF SOFTWARE

1.7.1 When permanently disposing of equipment containing storage media, all licensed software must be irretrievably deleted either before the equipment is moved off-site, or by utilising an approved 3rd party off-site service.

2. Responsibilities of Staff

2.1 College IT Manager

Responsibilities of the College IT Manager in respect of software licensing staff can be summarised as follows:

- Maintaining a University/College list of approved/supported software.
- Maintaining a University/College list of prohibited software.
- Maintaining a software inventory for the College (or Corporate Services).
- Maintaining copies of the software licences relating to the inventory.
- Ensuring that IT support staff carry out a regular automated audit of software in use on workstations.

2.2 IT Services Staff Authorised to Install Software

Responsibilities of IT Services staff authorised to install software in respect of software licensing can be summarised as follows:

- Ensuring, with the user, that software being used on the workstation is licensed, and approved/not prohibited.
- Ensuring, with the user, that they are complying with the conditions of the software licence.
- Ensuring that the installed software is recorded in the software inventory.

2.3 University Staff using Workstations

Responsibilities of University staff using workstations in respect of software Licensing can be summarised as follows:

- Ensuring that software being used on the workstation is licensed, and approved/not prohibited.
- Ensuring that they are complying with the conditions of the software licence.
- Disposing of redundant software appropriately.

GLOSSARY

Active Directory

Microsoft Active Directory software – the enterprise directory system used mainly for security.

Hardware

Computing and telecommunications devices including PCs, servers, routers, switches, disk units, modems etc.

Information Asset

An Information Asset is defined as a computer system, service, facility, application, software, data, database, proprietary knowledge, experience, insight, etc., which has value to the University. The term encompasses all information content that requires protection against security risks.

Information Assets governed by this Policy may legally belong to the University, or to a third party but placed in the University's care or custodianship (such as personal data).

Information Security

General term for the risk management activity involving the implementation, operation and maintenance of controls designed to meet business requirements for confidentiality, integrity and availability of information assets by preventing incidents and/or minimising impacts.

ISMS

Information Security Management System – the overall framework security comprising governance, policies, standards, procedures, guidelines, and other processes through which information security is directed and controlled.

ISSG

Information Security Steering Group – the University IT governance body responsible for information security.

Service

A defined set of functionality and information provided by one or more systems

System

A collection of elements organised for a defined purpose or objective. Systems consist of hardware, software, information, and human assets.

Workstation

An end-user computing device such as a PC, laptop, tablet or smartphone used to access resources over the University network.

APPENDIX A – DOCUMENTATION SCHEME

The following diagram shows an overview of the documents included within the Information Security Management System (ISMS).

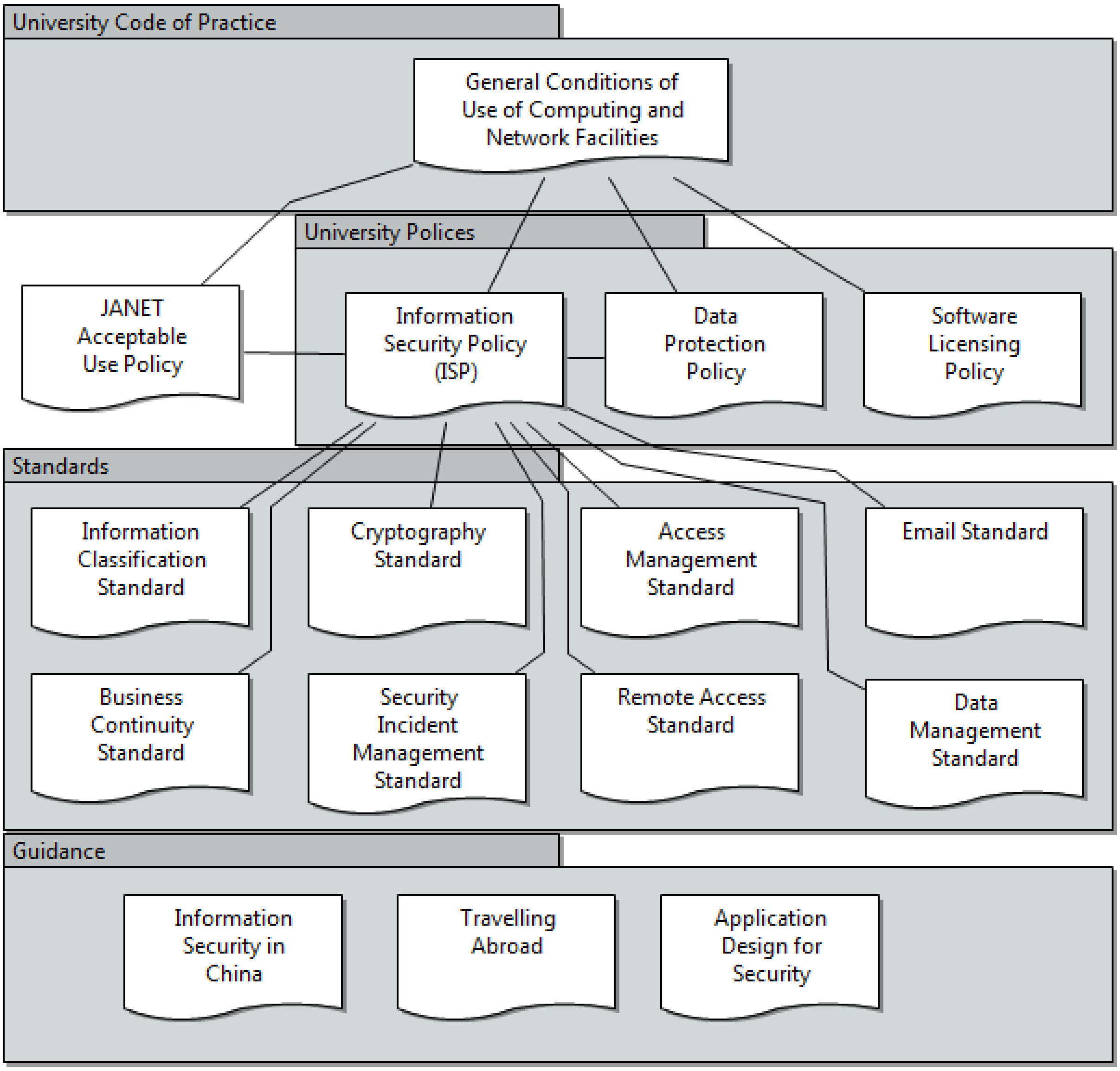
University Code of Practice
General Conditions of Use of Computing and Network Facilities
University Polices
JANET Acceptable Use Policy
Information Security Policy (ISP)
Data Protection Policy
Software Licensing Policy
Standards
Information Classification Standard
Cryptography Standard
Access Management Standard
Email Standard
Business Continuity Standard
Security Incident Management Standard
Remote Access Standard
Data Management Standard
Guidance
Information Security in China
Travelling Abroad
Application Design for Security

FIGURE INFORMATION SECURITY DOCUMENT SET