Information Security Policy

Staff Desktop

1 Introduction

1.1 The Information and Technology Services' (ITS) provision underpins many of the academic and non-academic activities of the University.

1.2 Suitable desktops are key to achieving these aims.

2 Background

2.1 ITS supplies a default Staff Desktop with the core software necessary for staff to undertake the majority of university business related processes. This model is known as the "Standard Managed" model and is judged by the University Information Services Committee to meet the needs of most staff.

2.2 When changes or additions to this core software are necessary, e.g. for new system releases or where the core software does not meet the requirements of the staff role, they are effected on a case by case basis by IT support staff.

2.3 Many settings on this "Standard Managed" desktop are unable to be changed and software cannot be installed by the user on their own. For staff roles where this provision does not meet their needs an alternative service is available. This service is known as the self-admin desktop.

2.4 There are some staff roles, identified by an information security risk analysis, which must use the default Standard Managed desktop model or a more restricted variant. Examples are given at Annex A.

2.5 Other units also supply desktops and this policy applies.

3 Purpose

3.1 Staff should be able to undertake their roles in an efficient and cost effective way.

3.2 The confidentiality, integrity and availability of corporate data and Institutional reputation are paramount.

3.3 Controls are in place to ensure the integrity of data and of the network and that software is licensed for use on Institutional Workstations.

3.4 The responsibility for the safety of Institutional data rests with senior post holders and may be delegated only by them. This is effected through the Information Services Committee.

4 Aims

4.1 To set standards for the provision of all university staff Desktops regardless of the unit that supplies them.

4.2 To provide the best computing environment for staff to undertake their roles.

4.3 To provide a consistent interface to corporate applications.

4.4 To ensure that corporate data is available only to those entitled to access it.

4.5 To ensure that corporate data is backed up on a regular basis.

5 Procedure

5.1 A member of staff requiring software or settings that cannot be supplied by the “standard managed” desktop should raise this with their line manager. The line manager will initiate the process to get authorisation to change to the self-admin desktop.

5.2 Should the changes incur costs, this must be authorised by the relevant budget holder.

5.3 The request is sent to the service provider. They will fulfil the request unless they believe that it needs to be raised with the Director of ITS.

5.4 If the request is raised with the Director of ITS and refused, then an appeal can be made to the Chair of the Information Services Committee.

6 Client responsibilities

6.1 Workstations will have mandatory settings that cannot or must not be changed e.g. anti-virus settings and software system patches.

6.2 It is the responsibility of the Delegated authorities to ensure that their staff meet their obligations under the service definition, most notably:

i) To abide by the IT Regulations and other policies, rules and regulations governing use of the network and the handling of information.

ii) To install only licensed software on the workstation.

iii) To save documents to a networked drive or other storage system compliant with the Information Security Policy and, exceptionally if data is kept on local storage, to make regular backup copies to media stored at a remote location.

iv) To keep mobile computing devices secured when unattended (e.g. to a desk, in a locked cabinet or stored in a locked car boot).

v) To undertake relevant training offered by ITS or the University for computer use.

ANNEX A

Some examples of staff roles that must use a managed model:

- Can change payroll details.
- Has direct access to the central University database.
- Has access to Special Category Data (as defined by the General Data Protection Regulation).

An example of a role which might have to use a managed model:

- Has access to confidential data (as defined in the Information Handling Policy).

Ownership:

Owner	Department/Team
Director ITS	ITS

Authors:

Author(s)	Department/Team
Jerry Niman	Consultant

Contributors and Reviewers:

Contributor/Reviewer	Department/Team
Matthew Trump	Information Service Assurance Manager

Revision History:

Version Number	Status D/R/A/I[1]	Date Issued	Reason for Issue	Issued by
2.1	R		Issued to ISC for Approval	PD
2.2	I	3 March 2015	Approved by ISC of issue	PD
2.3	I	20 June 2017	Minor Amendments	MT
2.4	I	12 June 2018	Minor Amendments	MT

[1] D = Draft; R= Ready for approval; A = Approved for issue; I = Issued