Information Security Policy

Systems Planning Policy

1 Introduction

1.1 This Policy sets out how Information systems are to be specified and designed and includes processes for identifying requirements and risks, designing appropriately configured systems to meet them and assigning responsibility for their security.

2 Objectives

2.1

2.2 To prevent unauthorised physical access, damage and interference to the

2.3 To prevent loss, damage, theft or compromise of assets and interruption to

2.4 To minimise the risk of system failures.

2.5 To prevent unauthorised access to operating systems and information held within information systems.

3 Scope

3.1 This policy applies to managers with responsibility for planning, procuring or commissioning of information systems.

3.2 Information systems should be understood to mean the critical information systems that serve the core purpose of the University, e.g. Library systems, Financial systems, Student systems, Research Systems, E-learning systems, Email, Web servers etc.

4 Policy

4.1 New information systems, or enhancements to existing systems, must be authorised jointly by the manager(s) responsible for the information and the Director of IT Services. The business requirements of all authorised systems must specify requirements for security controls.