Information Security Policy

Third Party Access to University Information Systems

1 Introduction

1.1 This policy sets out the conditions that are required to maintain the security of the University's information and systems when third parties, other than the University's own staff or students, are involved in their operation. This may occur in at least three distinct circumstances:

i) When third parties (for example contractors) are involved in the design, development or operation of information systems for the University. This might include the provision and installation of bespoke software, third party configuration maintenance or operation of systems or the outsourcing or partnering of an IT service or facility.

ii) When access to the University's information systems is granted from remote locations where computer and network facilities may not be under the control of the University.

iii) When users who are not staff or students of the University are given access to the University's information or information systems.

1.2 Each of these circumstances involves a risk to the University's information, which should be assessed before the third party is granted access. Any access granted via this policy must be subject to appropriate conditions and controls to ensure that the risk can be managed.

2 Objectives

2.1 To maintain the security of the University's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

2.2 To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles for which they are considered, and to reduce the risk of theft, fraud or misuse of facilities.

2.3 To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

2.4 To maintain the security of application system software and information.

3 Scope

3.1 The policy applies to managers responsible for the specification and approval of contracts for information processing or information processing systems that are undertaken by third parties, and to those responsible for the monitoring of such systems.

4 Policy

4.1 All third parties who are given access to the University of Sussex information systems, whether suppliers, customers or otherwise, must agree to follow the University's information security policies.

4.2 The University will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the University will require external suppliers of services to sign a confidentiality agreement to protect its information assets. Where personal information is involved, the supplier is required to incorporate the EU Data Protection Model Clauses in the contract; in addition where the transfer of data is to a region outside the EU the University will require the supplier to meet Privacy Shield standards or better.

4.3 Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of the University's information security policies.

4.4 All contracts with external suppliers for the supply of services to the University must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier or continent. Where the contract is for the supply or management of information services, the contract must include appropriate provisions covering:

i) Change control processes

ii) System administration processes

Capacity planning

iii) Authentication and authorisation mechanisms

iv) Time synchronisation

v) Session timeout

vi) Logging of privileged operations

vii) Processes for handling data subject access requests, responding to requests for information from law enforcement agencies and other third parties and for investigating suspected breaches of the University's or the supplier's acceptable use policies.

4.5 Any facilities management, service partner, or similar company with which the University may do business must be able to demonstrate compliance with the University's information security policies and enter into binding service level agreements that specify the means of demonstrating ongoing compliance with the University's information security policies, the performance to be delivered and the remedies available in case of non-compliance.

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
1.0	A	16/02/2010	Approved by ISC	
2.0	A	09/10/2014	Approved by ISC	
2.1	D	14/01/2015	'Personal information' qualifier added to 4.2. Detailed requirements for the provision of information services added to 4.4, 'ongoing compliance demonstration' requirement added to 4.5	JN
2.2	R	23/02/2015	Updated and issued to ISC for approval	PD
2.3	I	3/3/15	Approved by ISC for issue	PD
2.4	I	20 June 2017	Minor Amendments	MT

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