University of Liverpool

IT Procurement & Third Party Security Policy

(Procurement of IT Assets, Services and Release of University Owned Data)

Reference Number	CSD-017
Title	IT Procurement & Third Party Security Policy
Version Number	1.1
Document Status	Active
Document Classification	Open
Effective Date	04 March 2014
Review Date	28 March 2018
Author	Computing Services Department (David Hill)
Approved by	Corporate Services & Facilities Committee
Implemented by	Information Security Officer
Monitoring of compliance	Faculty Information Security Managers (Local) CSD Information Security (Central)
Comments	**This document should be read in conjunction with the University Procurement Policy** • **31/07/2015 Annual Review/Update v1.0 – 1.1** • **29/07/2016 – Annual Review** • **28/03/2017 – Annual Review**

IT Procurement & Third Party Security Policy

Table of Contents

1. Introduction

Information is a vital asset to any organisation, and this is especially so in the University which is a knowledge-driven organisation. Virtually all of our activities create information assets in one form or another.

2. Principles

The IT Procurement and Third Party Security Policy ensures that when the University makes use of IT services provided by an external agency that its information assets remain secure. The University has adopted the following principles which underpin this policy:

- All members of the University, who have access to information assets, have a responsibility to handle them appropriately and in accordance with their classification.
- Information asset owners are responsible for ensuring that the University classification scheme, which is described in the Information Security Policy, is used appropriately.
- University information assets should be made available to all who have a legitimate need for them.
- The integrity of information must be maintained; information must also be accurate, complete, timely and consistent with other related information and events.

3. Action Implementation

Procedures are in place to ensure the effective use of the IT Procurement and Third Party Policy. The following principles underpin these procedures:

- All service providers who have any access to the University's assets (information or equipment assets) must agree to follow the University's Information Security Management System (ISMS) at all times.
- University staff must assess the risk that assets may be exposed to by employing external IT service providers.
- All IT contracts with service providers must be monitored and reviewed to ensure that current University information security requirements are being satisfied.

4. Purpose

The IT Procurement and Third Party Security Policy sets out the conditions that are required to maintain the security of University assets via an IT procured and contracted service. IT services may be required to use, create, access and store University assets (information or equipment).

5. CSD Managed Services

CSD will be the point of contact for all University managed services and centrally managed IT assets. For more information on CSD services, please refer to Computing Services Department homepage.

6. CSD Preferred suppliers and Specialist IT Services

For more information on the CSD preferred supplier list, please refer to the University supplier's guide.

If the specific IT service you require is not listed within the University supplier's guide, contact the CSD Service Desk. Examples of specialist IT services include:

- Financial/payment systems
- Network equipment and software
- Database/server/storage solutions

IT services that are provided and managed by CSD include provision of support for that service or IT asset. Examples include:

- Resource and day-to-day management of the procured service/IT asset
- Training and skills to be able to manage the procured service/IT asset
- Incident Response Management

7. Non CSD IT Services (Unsupported Services)

CSD operates to provide IT services to all members of the University and will provide support to staff when selecting third party suppliers. CSD should be contacted in the first instance before making any approaches for IT services to a third party.

If services are not in accordance with University policies and standards, this may delay/defer the required CSD support.

8. Security Review (Pre Contract/Agreement/Collaboration)

All IT services must have a risk assessment undertaken and the risks mitigated prior to the services being adopted.

CSD will assist staff with risk management and decision making as part of the following activities:

- Awarding IT service contracts/collaboration
- Reviewing arrangements with new or existing IT service providers/collaborators – for example, to ensure what they "say" and "do" is evidenced
- Understanding how University assets will be managed and secured on a day-to-day basis
- Releasing University information assets

Releasing University Information Assets/Identifiers

Any University owned data and identifiers that relate to staff and/or student(s) that is required for third party collaboration must be reviewed prior to release. The University has a legal obligation to ensure the protection and security of personal data.

Data Sharing – Identifiers that could be communicated following review **The identifiers below are subject to a formal review prior to sending to a third party or collaborator. It is dependent on the nature of use; whether there are other means of collecting the data; and whether it is required for critical University systems and operations.**	**Data Sharing – Identifiers NOT to be communicated** **These identifiers must NOT be communicated publically and/or transferred to third parties as part of external collaborations due to legislation and general security of University systems and data.**
ID/ Username	Gender
First Name	Marital Status
Last Name	Ethnicity
University Contact Phone Number (Mobile/Landline)	Religion
University Email Address	Sexual Orientation
	Country of Nationality
	Health Records/Disability
	Address
	Date of Birth (DOB)

***N.B. These identifiers are not an exhaustive list and are subject to change dependent on University systems and controls.**	Pin/Password
	Payroll Number(s)
	National Insurance Number(s)
Important! Data/Identifiers must NOT be given out unless disclosure has been agreed/given by the University and consent from staff and students has been given and can be evidenced.	

Table 1 – University collected/owned data and identifiers

Service Provider Security Review/Data Exchange Agreement

All University assets, to which a service provider/collaborator has access or wishes to have access, must be handled in accordance with procedures which satisfy legislative, regulatory and University risk and security management activities. The details of these procedures will depend on the nature of the data and identifiers required for that service.

The table below shows the types of reviews, services and documents that help staff in appointing a collaborator and/or service provider.

Pre – Contract/Collaboration Pre-Release of Data/ Risk Review	**Completion of Risk Review/Mitigation and Appointment**	
Service Provider Security Review (SPSR)	Data Exchange Agreement	Formal Contract
University staff who are authorised and responsible for appointing service providers/collaborators or release of University assets must complete a Service Provider Security Review (SPSR) prior to awarding/appointing a contract/agreement of work or releasing data.	Whereby all risks identified within the initial SPSR assessment have been mitigated appropriately.	Where formal contracts are required or for advice, restrictions and boundaries of a formal contract please refer to the Procurement Team in the first instance.
The SPSR should be completed and sent to the Information Security Officer as soon as possible to ensure the risk assessment can be undertaken appropriately.	Where a formal contract is not required the staff member must ensure that a data exchange agreement has been signed and accepted by the collaborator/service provider.	
Failure to send the completed SPSR within a reasonable timescale may delay/defer Information Security completion and to the risk assessment/project.	Advice and guidance from Legal, Risk and Compliance Team and/or the Data Protection Officer should be sought in the first instance.	
For more information please refer to the Information Security Officer: **Servicedesk@liverpool.ac.uk**	For more information please refer to the Data Protection Officer	For more information please refer to the Procurement Team.

Table 2 – Professional Services Review (SPSR/Data Exchange Agreement and Formal Contract)

Compliance and Certification

CSD evidential requirements for IT service providers include, but are not limited to:

- ISO27001 Compliance/Certification
- PCI-DSS Compliance/Certification
- Data Protection Registration Number/Association
- ADISA Registration (Asset Disposal and Information Security Alliance)
- Evidence of Information Security Framework and documentation
- Evidence of workings with specific standards/associations/controls of security industry bodies e.g. ISACA, CESG, COBIT, CPNI and ITIL.

Where evidence of compliance and certification cannot be established, the University, as part of its review and continuous improvement activities, must undertake an assessment of the third party controls prior to allowing access to University assets.

In the event that compliance and certification cannot be evidenced, other mitigating controls should be evidenced from the service provider, for example:

- Personnel background checks e.g. DBS and CCJs.
- Protection of data methods (both physical and technical)
- Incident/Business Continuity/Disaster Response Plans
- Terms and Conditions of support services
- JISC/JANET/University SIG (Special Interest Group) recommendations

9. Information Security within Contracts (Appointment of a Service Provider/Collaborator)

University staff, responsible for agreeing IT Service contracts must ensure that the terms and conditions do not contravene the University's Information Security Management System (ISMS), Procurement Policy , procedures and supplier code of conduct. In any event all contractual documents must be forwarded to the Procurement Department for vetting prior to signature by an authorised officer of the University.

All University contracts must ensure boundaries of undertakings and protection of University assets for the full duration of the contracted services. Contracts and services must:

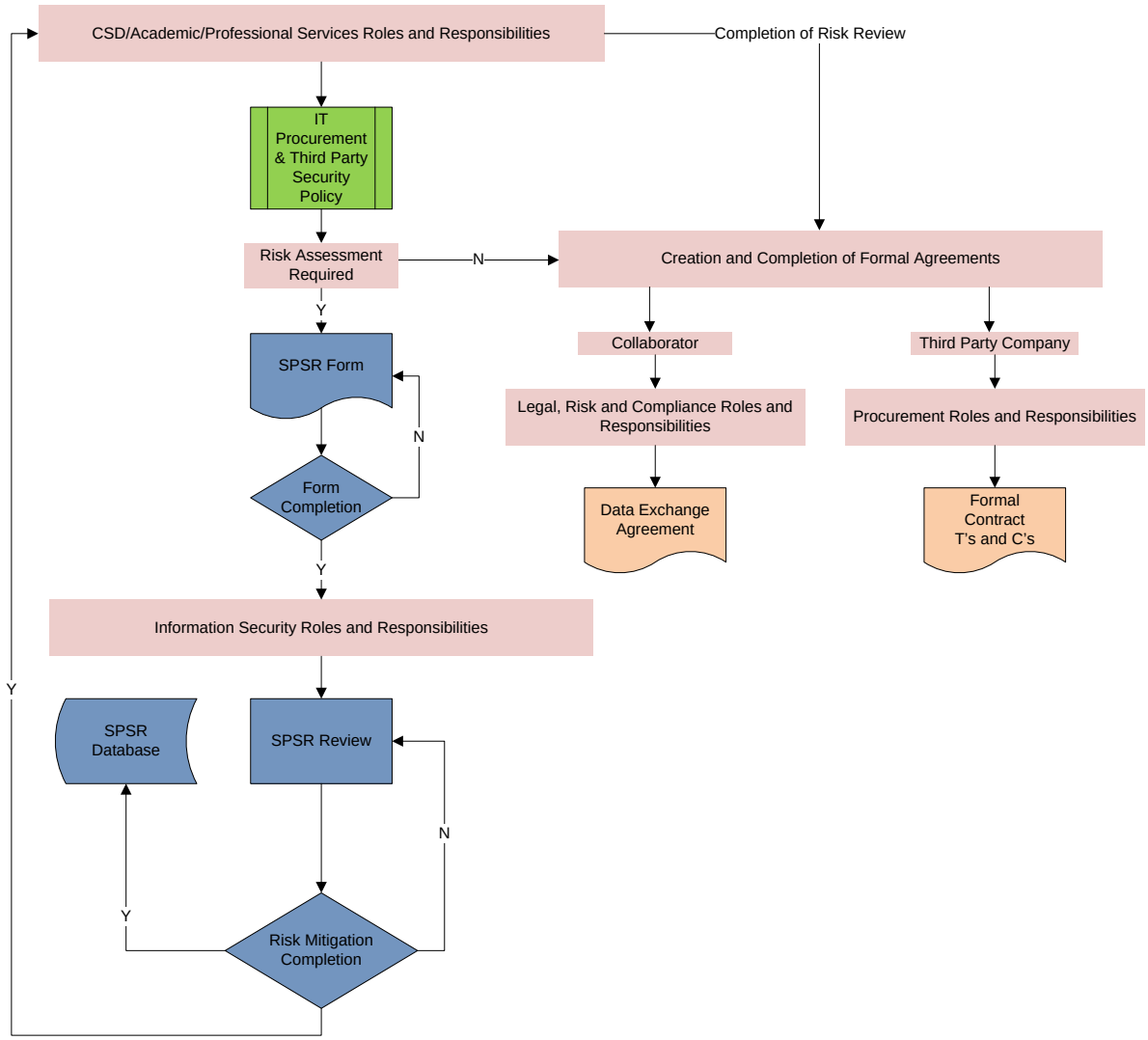
- Be monitored and reviewed annually to ensure that information security requirements are being satisfied.
- Include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.
- Be able to demonstrate compliance with the University's ISMS (Information Security Management System).
- Include specific acceptance of the University ISMS.
- Include an undertaking that University assets will be retained or transferred to the University upon completion of contracted works and that any sensitive data will be removed from the service provider's data sources.
- Ensure the contract/agreement states University data being transferred will only be used for the purposes of the collaboration and no data will be transferred to any third parties for any other purposes.
- Include a right to audit. The University must ensure the right to audit is agreed with the contracted service prior to acceptance of the contract.

10. Service Provider/Collaborator Relationship Management

It is imperative that the University and its appointed service provider/collaborator understand the University's positioning of continuous improvement.

Regular Compliance and Monitoring must be undertaken by the University with regards to its assets. For more information please refer to the Information Security Review Policy.

11. Service Provider Security Review (Process)



12. Service Provider Security Review (Roles and Responsibilities)

Source/Requestor

It is the responsibility of the University member to ensure that the Service Provider Security Review Form is completed before sending for information security input. Failure to supply all relevant information may delay the process.

Upon submission of the SPSR it will be the responsibility of the requestor to call for further input from the Legal, Risk and Compliance and Procurement teams as required.

Information Security

The Information Security Officer will undertake a security review of the information provided within the SPSR. The information Security Officer will consult and advise on the potential risks and threats to the University and its assets, with mitigating and follow up actions required, if necessary.

13. Technical Security Review (Testing and Assessment)

If sensitive University assets (Confidential/Strictly Confidential) are involved, this may require technical security assessments to be undertaken **prior** to introducing new services to the University IT environment.

Appropriateness and CSD Support (Core Network Infrastructure)

To ensure procured IT services are "fit for purpose" and do not pose a risk to the University and its core network infrastructure, University staff must engage with CSD for technical input and guidance in advance of any work.

14. Transfer/Security of University assets

Any assets created, used, accessed, processed, managed and stored by the service provider/collaborators (including any third-party contractors, subcontractors or other entities hired by the awarding service provider, as part of a University IT development or service), which are considered to be the property of the University, must be:

- Securely transferred to the University
- Securely removed from non-University data sources

Please refer to the Information Asset Classification Policy for more information on the classification of University assets.

15. Dispute

In the event that there is a dispute between the IT supplier and the University, the University may require that assets are placed with an approved escrow service provider, until a resolution between the University and service provider has been completed.

Please refer to the Legal, Risk and Compliance Team for more information.

16. Security Incident Response

Should the service provider encounter any security risks or threats that may impact the confidentiality, integrity and availability of University assets, they must inform the University within a reasonable timeframe to allow the University to undertake necessary remedial action.

Please refer to the Information Security Incident Response Policy for more information.

17. CSD Service Desk Contact Details and Service Times

Contact details and opening hours of the CSD Service Desk are available via:

- Logging an online support request: http://servicedesk.liverpool.ac.uk/
- Email: servicedesk@liverpool.ac.uk
- Telephone: 44567 (internal)
- Telephone: +44 (0) 151 794 4567 (external)

18. Freedom of Information Request (FOI)

Any information requested by an unapproved authority, third party or member of the public under the Freedom of Information Act is to be referred to the University Legal, Risk and Compliance Department in the first instance. Legal, Risk and Compliance will ensure all requests are responded to within the agreed timeframe and within the structured process set by the Information Commissioners Office (ICO). For more information please refer to the Freedom of Information Publication Scheme.

19. Legal obligations and University policies

This policy is aimed at all members of the University who have a responsibility for the use, management and ownership of information assets. This policy is part of the University Information Security Management System (ISMS) and should be read in conjunction with the **Information Security**

Policy and its sub policies and relevant UK legislation. Further relevant policies and legislation are listed in **Appendix A**.

20. Compliance and Monitoring

All members of the University are directly responsible and liable for the information they handle. Members of staff are bound to abide by the University IT regulations by the terms of their employment. Students are bound to abide by the University IT Regulations when registering as a student member of the University.

Authorised members of the University may monitor the use and management of information assets to ensure effective use and to detect unauthorised use of information assets.

Appendix A – University ISMS Reference

- Regulations for the Use of IT Facilities at the University of Liverpool
- JANET Acceptable Use policy
- Information Security Policy
- Workspace and IT Equipment Security Policy
- Information Security Incident Response Policy
- Information Asset Classification Policy
- Information Security Review Policy
- Security Investigation Policy
- Procurement Policy
- Data Protection Policy
- Freedom of Information Policy
- Copyright Policy
- Card Payment Policy
- Records Management Policy
- Records Retention Policy
- Risk Management Policy
- Student/HR Disciplinary Procedures

Relevant legislation includes:

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Data Retention Investigatory Powers Act 2014
- Counter Terrorism and Security Act 2015 (Prevent)
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002

Relevant Regulation includes:

- PCI-DSS (Payment Card Industry Data Security Standards)