University of Bristol
Information Security Policy

Title:	**Outsourcing and Third Party Compliance Policy**
Reference:	**ISP-04**
Status:	**Approved**
Version:	**1.4**
Date:	**July 2013**
Reviewed:	**August 2019**
Classification:	**Public**

Contents

Introduction

This Policy is a sub-policy of the Information Security Policy (ISP-01) and outlines 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.

Scope

This policy applies to any member of the University who is considering engaging a third party to supply a service where that service may involve third party access to the University's information assets. This policy does not cover the individual sharing of documents and information by members of staff and students with third parties, colleagues should review the Information Handling Policy (ISP-07) in this instance. Its purpose is to inform readers of the risks and expectations on them when outsourcing or allowing third party access to information systems. This third party access could occur in a number of scenarios, common examples being:

- The use of cloud computing services;

- When third parties are involved in the design, development or operation of information systems for the University;
- When third party 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;

Managing outsourcing risk

Prior to outsourcing or allowing a third party access to the University's non-public information or systems, a decision must be taken by staff of appropriate seniority that the risks involved are clearly identified and acceptable to the University. The level of staff seniority will depend on the nature and scale of the outsourcing. Advice must be sought from the Secretary's Office and Procurement during the decision making process.

Formal outsourcing

Where a service is formally outsourced by the University, the process must be managed by the relevant University staff and a contract must be in place that covers standards and expectations relating to information security (see 'Contractual issues').

Due diligence

The process of selecting a third party service provider must include due diligence of the third party in question, a risk assessment and a review of any proposed terms and conditions to ensure that the University is not exposed to undue risk. This process may involve advice from members of the University with expertise in contract law, IT, information security, data protection and human resources.

This process must also include the consideration of any information security policies or similar information available from the third party and whether they are acceptable to the University.

Contractual issues

All third parties who are given access to the University's non-public information or systems must agree to follow the information security policies of the University. Advice should be sought from the Secretary's Office and/or Procurement in relation to contractual arrangements.

Confidentiality clauses must be used in all contractual arrangements where a third party is given access to the University's non-public information.

Contracts must also contain the support arrangements with third parties, especially in the event of a security breach. These will include hours of support, emergency contacts and escalation procedures.

Use of third party services must not commence until the University is satisfied with the information security measures in place and a contract has been signed.

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.

Data Protection Act

A Privacy Impact Assessment (PIA) must be completed at the outset of any project that will potentially involve personal data being accessed by a third party. Any outsourcing arrangement involving the transfer of personal data to a third party must include the acceptance of the University's standard personal data processing terms.

If the outsourcing involves the transfer of personal data outside the European Economic Area (EEA), it must only be to a country or territory that ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The Information Commissioner's Office (ICO) provides a list of countries it has deemed to provide an adequate level of protection. If the transfer is to the USA, the company or organisation must be signed up to the US-EU Privacy Shield scheme (or equivalent) for the duration of the contract.

The University's Data Protection Policy can be found here:
http://www.bristol.ac.uk/secretary/data-protection/policy/

Informal outsourcing

There are extensive IT services that are available to members of the University via the internet which the University will have no formal agreement or contract in place with - examples include email services and cloud storage providers. Users of such services are required to accept the provider's set terms and conditions and the University has no ability to negotiate as it would via the formal outsourcing procedure.

The use of such services for storing University information present a real risk to the University as there is no way the University can ensure the confidentiality,

integrity and availability of the information without a formal agreement in place. The storage of personal data with such providers is likely to be a breach of the Data Protection Act for which the University could be penalised by the Information Commissioner.

In light of these risks, wherever possible, University staff must only use services provided or endorsed by the University for conducting University business. The University recognises, however, that there are occasions when it is unable to meet the legitimate requirements of its members and that in these circumstances it may be permissible to use services provided by other third parties.

University data which is subject to the Data Protection Act or which has a classification of confidential or above must be stored using University facilities or with third parties subject to a formal, written, legal contract with the University. Those wishing to engage third parties in this way must have a Data Processing Agreement in place before data is transferred.

In cases where it is necessary to remove data from the University, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Further advice is available from IT Services and/or the Secretary's Office.

University staff must not configure their University email account to automatically forward incoming mail to third party services with which the University has no formal agreement.

Third party physical access

A risk assessment must be completed prior to allowing a third party to have access to secure areas of the University where confidential information and assets may be stored or processed. This assessment must take into account:

- what computing equipment the third party may have access to;
- what information they could potentially access;
- who the third party is;
- whether they require supervision;
- whether any further steps can be taken to mitigate risk.