University of Bristol
Information Security Policy - Outsourcing and Third Party Compliance

Title	Outsourcing and Third Party Compliance
Reference	ISP-04
Status	Approved
Version	3.0
Date Created	July 2013
Last Reviewed	October 2023
Next Review	October 2024
Classification	Public

Contents

1. 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 data and systems when third parties, other than the University's own staff or students, are involved in their operation.

2. 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's purpose is to inform readers of the risks and expectations on them when outsourcing or allowing third party access to information systems. 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) for more information about this.

Third party access could occur in various scenarios, common examples being:

- The use of cloud computing services (such as cloud hosting and processing) or other third-party software services and web applications.

- 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.

3. Policy

3.1. Managing Outsourcing Risk

Before outsourcing or allowing a third party access to the University systems or University data classified as Open or above, 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 classification of the data involved (as per University Information Classification Scheme) and the value and complexity of the contract. Advice must be sought from Information Security, the Legal Services and Secretariat and Procurement during the work request approval process.

3.2. Formal Outsourcing

Where a service is formally outsourced by the University, the process must be managed by the relevant University staff and a contract that covers standards and expectations relating to information security (see '3.4 Contractual Considerations') must be in place.

3.3. 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, or engaged external professionals, 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.

3.4. Contractual Considerations

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 third parties that are given access to the University systems or University data classified as Open or above must agree to follow the University's information security policies, or the terms set out in any agreed deviation from those policies with appropriate University signoff.

Advice should be sought from the Legal Services and Secretariat and/or Procurement in relation to contractual arrangements. University standard terms should be used where possible: Standard Terms and Conditions for the Supply of Goods and Services.

Confidentiality clauses must be used in all contractual arrangements where a third party is given access to the University data classified as Open or above.

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

Contracts must include provisions to ensure the continued security of data and systems if a contract is terminated or transferred to another supplier.

All contracts for the supply of services to the University by external suppliers must be monitored and reviewed to ensure that information security requirements are satisfied.

3.5. Data Protection Act

The Data Protection Impact Assessment (DPIA) screening process must be completed at the outset of any project that will potentially involve data classified as Confidential and above being accessed by a third party. Any outsourcing arrangement involving the transfer of data classified as Confidential and above to a third party must include the acceptance of the University's standard personal data processing terms or a negotiated equivalent incorporating the same standards. All contracts that require the processing of personal data must have an agreed purpose and lawful basis for processing that data.

If the outsourcing involves the transfer of personal data outside the UK to a country or territory that the UK recognises ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data, then transfers can take place without any further authorisation (Art.45 UK GDPR). The Information Commissioner's Office (ICO) provides a list of countries it has deemed to provide an adequate level of protection. If the outsourcing involves the transfer of personal data outside the UK to a country or territory that the UK does not recognise as providing an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data, then the UK International Data Transfer Agreement (IDTA) or the Addendum may be used as a contractual transfer tool to comply with Art.46 UK GDPR when making personal data transfers. Guidance on the appropriate use of the IDTA should always be sought from the University's Data Protection Officer.

The University's Data Protection Policy: https://www.bristol.ac.uk/secretary/data-protection/policy/

3.6. Informal Outsourcing

There are extensive online IT solutions 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 cannot negotiate as it would via the formal outsourcing procedure.

The use of such services for storing and/or handling of University data presents a 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 data classified as Confidential or above 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. In these circumstances University members are expected to engage with IT Services and Procurement to begin the required due diligence (see section 3.4). Third party terms and conditions must not be accepted prior to the completion of this approval process.

For further guidance on placement of University data on non-University systems refer to the Removal of Information section of the Information Handling Policy (ISP-07).

University data subject to the Data Protection Act or that 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.

3.7. 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 potentially could have access to;
- what information they could potentially access;
- who the third party is;
- whether they require supervision;
- whether the third-party access request places other existing contractual terms at risk;
- whether any further steps can be taken to mitigate risk.

4. Further Guidance

- Information Handling Policy (ISP-07): https://www.bristol.ac.uk/infosec/policies/information-handling-policy/
- University Information Classification Scheme: https://bristol.ac.uk/media-library/sites/infosec/documents/Information Security Classifications.pdf
- Procurement Policy: https://uob.sharepoint.com/sites/finance-services/SitePages/procurement-policy.aspx
- University Standard Terms and Conditions for the Supply of Goods and Services: Procurement | Directory of Professional Services | University of Bristol
- The University's Data Protection Policy: https://www.bristol.ac.uk/secretary/data-protection/policy/
- Data Protection Impact Assessment (DPIA): https://www.bristol.ac.uk/secretary/data-protection/guidance/privacy-impact-assessment/
- Information Commissioner's Office (ICO): https://ico.org.uk/