Third Party Supplier Security Management Policy v1.0

Organisation	Oxford Brookes University
Title	Third Party Supplier Security Management Policy
Creator	IT Services
Approvals required	CIO; VCG
Version	v1.0
Owner	Head of Information Security Management
Subject	Information Security Management
Rights	Public
Renewal date and responsibilities	Annually by the Information Security Working Group. Drafted on 24 October 2018

Revision History			
Date	Author	Version Number	Comments
11/11/18	Gareth Packham	v0.1 (draft)	Initial draft
17/03/19	Gareth Packham	v1.0 (live)	Minor amendments only

1. Purpose

The objective of this Policy is to protect any information assets or data belonging to Oxford Brookes University to which third party supplier access (or potential access) is given. Compliance with this Policy contributes to the University meeting its governance requirements, including compliance with the Data Protection Act 2018, the General Data Protection Regulations and the ISO27001:2013 information security management standard.

2. Scope

2.1 This Policy sets out the requirements which must be adhered to when engaging any third party which has access to any information assets or information which belongs to the University and how the University will monitor compliance. It covers the supply of goods and services including the appointment of contractors.

Arrangements

2.2 This Policy applies to any type of contractual or other arrangement (agreement/s) where there is data processing or access to critical systems which support the data processing functions of the University.

Examples of arrangements include:

- commercial and non-commercial activities
- administration carried out directly for the University, including any affiliates or partners, or by the University on behalf of another organisation.

An information asset is any data, device, or other component of the environment that supports information-related activities and has a value to the University. (The value may be financial or be relevant to the reputation of the University for example.) Information assets include databases, electronic file storage, web platforms and personal computers as well as documents, filing cabinets and premises. Examples of critical systems affected by this Policy are:

- Student record systems
- Human Resources systems
- Finance systems
- Incident reporting systems
- ICT network systems

These arrangements may be evidenced by procurement documentation; contracts; information sharing agreements; confidentiality agreements; licences; or otherwise.

Data

2.3 The Policy applies to all data in the scope of 2.2 above.

This includes:

- Personal Data
- Special Category personal data
- Commercial or non-commercial data irrespective of its format (digital or paper).

This policy applies equally to Confidential, Restricted or Public Data (as defined in the Oxford Brookes Information Classification Policy).

Staff

2.4 The Policy applies to all staff including: contractors, temporary staff and third parties employed directly and indirectly by the University and any third party (to include subcontractors and affiliates) which may or does enter into an Arrangement with the University. Staff acting for and on behalf of the University and staff acting for and on behalf of any Third Party are responsible for ensuring the implementation of this Policy.

2.5 The Policy should be brought to the attention of any Third Party by the University during any procurement exercise or whenever an arrangement is entered into when the Policy has application. It should form part of the procurement and supply/purchasing procedure of the University.

3. Context

3.1 In the unlikely event of a conflict between a contractual, policy or other requirement, the conflict should be raised with both IT Services and Legal Services for resolution.

3.2 The Policy should be adhered to in conjunction with other relevant Brookes' policies as well as any other relevant Regulations, Guidance, law, protocol or Agreement contractual or otherwise (such as procurement requirements) applicable to any arrangement. The University Regulations can be found at www.brookes.ac.uk/regulations and the IT policies can be found at
www.brookes.ac.uk/it/information-security/policies-procedures-legislation

There may be industry best practice or other requirements which must be adhered to. Relevant legal provisions include, but are not restricted to: procurement, data protection, health and safety.

3.3 The requirements of the Policy subsist until any procurement exercise or arrangement is ended, subject to any legal, policy (such as data retention periods) and other requirements (such as contractual or licence provisions).

4. Access Control

Identification and control of risk by assessment

4.1 The University will assess the risks posed to any information, information assets or system posed by allowing third parties access or involving third party suppliers.

4.2 As part of the risk assessment, the University will define the different types of information access that a supplier will be allowed. This is restricted to what is required to complete the task ('data minimisation').

4.3 Any third party allowed access to University systems, information assets or data will be given details of how their access will be audited and controlled in accordance with policy such as the Access Control Policy found at
www.brookes.ac.uk/it/information-security/policies-procedures-legislation/

5. Risk Management

5.1 All third parties who are given access to the information, information systems or information assets belonging to the University must agree to demonstrate compliance with all relevant information security policies, guidelines and procedures, as well as the law.

5.2 University staff within the Faculties and Directorates (in conjunction with IT Services where appropriate) will assess and record any risks posed to its Information Assets and from business processes involving third parties. Any identified risks must be documented and efforts made to minimise that risk and/or determine if it is acceptable to the organisation.
Where a third party is processing significantly large volumes of personal data or other high-risk data processing a Privacy Impact assessment should be completed in addition to a standard information risk assessment.

5.3 Records of identified risks must be reviewed during the lifetime of the arrangement with the third party in the event that there is an indication that the exposure to risk may or have changed. Any reviews and outcomes must be recorded.

5.4 Oxford Brookes University will determine the level of access as well as the duration of access that third parties may have to Information Assets and Critical Systems based in part on the identified risks as well as any other relevant factors.

5.5 On written request, the third party must provide details of organisational and technical security controls in use which are relevant to the data processing or access.

5.6 The third party shall ensure that the University Information Assets Information and critical systems are appropriately protected and that this is monitored to prevent unauthorised access or use of University information assets.

6. Legal Requirements and written agreements

6.1 The University must consider whether it is appropriate to complete a Privacy Impact Assessment to determine whether information sharing is lawful for new projects and procurement exercises.

6.2 Any supplier of a pre-defined critical system must sign and adhere to the Information Security Agreement or contract in place for suppliers.

6.3 An Information Sharing Agreement should be completed where there are regular or significant quantities of data being shared with a third party to document the process, unless this is explicitly covered in a written contract. Information Sharing Agreements should be approved by both the IT Services Information Security team prior to authorisation and signing via Legal Services.

6.4 Contracts should cover all appropriate information sharing and security arrangements and requirements. Please see appendix 1 for further details.

6.5 The University is required to consider the legal basis for sharing personal data with any third party and record the same. If the ground for sharing personal data is found to be because it is in the legitimate interests of the University then a legitimate interests assessment should be completed by the IT Services Information Security team.

6.6 Permission to access Information Assets or business processes can be agreed in the absence of appropriate and satisfactory compliance with this policy in the event of an emergency, exceptionally, or where this is agreed as genuinely impractical by the Vice Chancellors Group or a Director / Head of Department (advice and guidance to be provided by IT Services Information Security team).

6.7 Compliance should be recorded by the University. If advice or support is needed to confirm what is required in any given situation please contact info.sec@brookes.ac.uk

7. Human Resources Security

Pre - employment screening for third parties, sub -contractors and affiliates

7.1 The third party is responsible for ensuring that the information security roles and responsibilities of all third parties and any subcontractors or affiliates are clearly defined and documented and that this information can be made available to the University where required.

7.2 The third party can show that, at their own cost, all appropriate pre-employment checks have been carried out. This includes: checking references, qualifications, appropriate financial probity and criminal conviction and rights to work checks (when it is both lawful and

appropriate that these should be carried out). All staff must have the pre-requisite skills and qualifications and training for a given role.

During employment

7.3 The third party can show that their staff are:

- subject to suitable and comprehensive induction requirements
- have access to any ongoing training covering information security and any other issues relevant to the role
- subject to codes of conduct protect any information or information assets belonging to the University. These codes of conduct incorporate sanctions when necessary.
- compiling a complete asset inventory which is available for inspection
- ensure staff are complying with access and security requirements (including ID passes etc.)

7.4 The third party shall consult with the University prior to the event of any personnel changes.

Termination of employment

7.5 The third party will follow the University's policies at termination or suspension of employment to ensure that access to secure premises systems or information assets are terminated appropriately and access is denied promptly.

8 . Review

8.1 (a) The responsibility for managing supplier relationships must be assigned to an designated individual or team.

8.1 (b) In conjunction with the University the third party must also identify a designated individual or team to manage the contract and and be:

- prepared to be audited in accordance with University requirements (as defined by policy and relevant legislation)

- monitor contract performance levels to verify adherence to any agreements

- provide information/audit data about any security incidents (or near misses)

- preempt, identify and resolve problems by anticipating security events and operational problems as well as learning from experience

- ensure that the third party maintains a sufficient service capability and workable plans to achieve the contractual requirements and maintain business continuity.

Other obligations

Malware and data security protection

8.2 In the event that the third party has reason to be concerned about any actions of their employees, or the procedures in place, that could compromise the confidentiality, integrity or security of the information or information assets belonging to the the University then the third party will advise the University immediately.

8.3 The third party will notify the University immediately if it becomes aware of any malware or security concerns relating to their own systems which have not been automatically corrected or quarantined and shall provide written details of protective measures taken.

8.4 Any “near miss” or actual data protection breaches which could or did compromise the confidentiality integrity or security of University Data must be reported by the Third Party to the IT Services Information Security Team at once on info.sec@brookes.ac.uk.

9. Third party supply chains

9.1 The third party must supply full details of any subcontractors that it intends to use in the provision of services prior to engagement.

9.2 In addition to providing the company name, address and location of the company, it is the responsibility of the the third party to ensure that:

- the subcontractor has entered into any of the prerequisite written agreements required by the University
- any subcontractor complies with the same requirements as the third party
- the third party must check that these requirements have been fulfilled
- the third party must provide both the assurance and evidence requested by the University as the law allows and the University requires
- the third party must complete an information security risk assessment to the satisfaction of the University prior to allowing access to the subcontractor to any of the University’s Information Assets systems or information
- the third party will conduct security reviews on any subcontractors at the instigation of the University or in any event in accordance with contractual requirements.

10. Managing changes to supplier services

10.1 Mechanisms must be in place to manage changes to supplier services when changes can occur.

10.2 The risk assessment carried out at procurement stage should cover the implications of any changes of supplier services and needs to be revisited during the lifetime of the contract. Where services are critical, how to manage those changes must be addressed as part of business continuity planning.

Monitoring review and auditing third party contracts

10.3 Oxford Brookes University must regularly review and audit service delivery to ensure that changes with supplier services are managed. This is to protect both normal business and business continuity in every day and exceptional circumstances. The frequency of the monitoring needs to be fixed at procurement stage and it will depend on the goods and services provided as well as the proposed duration of any arrangement. Any audit findings should be recorded, this should include how any non-conformities or areas of non-compliance which are identified will be addressed including agreed remedies and timeframes.

10.4 Another function of the review / audit is to provide updates about any information security incidents and these must be reviewed in the light of any legal requirements (There may be separate contractual consequences, investigations or other legal remedies which could arise out of any findings).

11. Cost of compliance

11.1 Suppliers and third parties need to manage any additional costs in relation to compliance. This includes any Third Parties' obligations under data protection law, or risk assessment. The University is not expecting to warrant or indemnify against any possible breach of data protection law by third parties.

10.2 The University is not expecting to accept contract/agreement price increases from suppliers, should new systems or processes be required to implement the policy or Legislation.

Appendix 1

This is the checklist to be used by the IT Services Information Security Team in conjunction with the procurement team and legal services, to make sure that any proposed contract or information sharing arrangement is compliant with this policy, data protection principles, laws and ISO27001:2013:

Compliance with General Data Protection Regulation Principles:

Is the personal data in scope:

a) *Processed lawfully, fairly and in a transparent manner in relation to the data subject.*

- identify lawful basis of processing (including special category data)
- if processing using 'consent' is it freely given, unambiguous and informed?
- if processing using 'legitimate interests' has a legitimate interest assessment been completed?
- will the data subjects have a reasonable expectation that data will be processed in this way. Is processing covered by existing privacy notices? If not, check if the existing privacy notices need to be amended.
- does the project / process involve any international data transfers? If yes, do they meet GDPR requirements?

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) Accurate and, where necessary, kept up to date.

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed:

- does personal data in scope need to be retained for defined statutory period?
- if not, how is operational necessity defined?

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- Is the supplier / partner ISO27001 certified?
- If not what other evidence can they provide of information security best practice?
- Are data flows to and from Brookes secure?
- Are operational security controls adequate?

Third Party Processor Contract Compliance

GDPR Article 28 Requirement	Compliant?	Reference
Processes the personal data only on documented instructions from the controller		
Ensures that persons authorised to process the personal data have committed themselves to confidentiality		
The processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk		
Ensure any subcontractors meet GDPR requirements for processors		
Assist the controller in fulfilling its obligation to respond to requests for exercising the data subject's rights under GDPR		
Notify the controller of any personal data breach and assist the controller in fulfilling its own obligations regarding breaches		
Delete or return all personal data to the controller upon request		
Makes available to the controller all information necessary to demonstrate compliance with their obligations under GDPR		

Any contract must make reference to:

- a right to audit
- prompt notification about security breaches
- adherence to security practices
- response time to vulnerabilities
- Management of supplier's supply chain risks - consent in advance from the University must be secured before a third party can be included in the supply chain
- How the Oxford Brookes University will be informed regarding changes in its environment that may impact the Brookes business and how services will be maintained.

Appendix 2

This checklist sets out the minimum requirements that must be met by a third party supplier.

	GENERAL REQUIREMENTS
	There must be a written contract/information sharing agreement/non disclosure agreement etc. in place.
	Any arrangement requires any staff with access to data to adhere to information security policies and any other requirements imposed by Oxford Brookes University (relevant policies should be provided to the proposed supplier at procurement stage.)
	HUMAN RESOURCES
1.	A suitable induction and refresher training programme must be in place to cover information security and data protection.
	PHYSICAL AND ENVIRONMENTAL SECURITY
2.1	An appropriately secure governance structure must be available (is there any external validation such as ISO27001?)
2.2	Physical access must be in place to control access (signing in procedures, cctv where appropriate, secure server rooms, alarms.)
	ACCESS SECURITY
3	System and administrative accounts must have the capability to be changed without resulting in changes to software coding.
	NETWORK AND INFRASTRUCTURE SECURITY
4.1	An appropriately secure infrastructure must be available (is there any external validation such as ISO27001?)
4.2	Networks hosting Oxford Brookes University data must be secure; either there must be physically separate networks which are appropriately protected or logical networks should be used with suitable protection.
4.3	Suitable management procedures must be in place to ensure security for patches.
4.4	The supplier must use effective anti-malware and other protection; consideration must be given to the use encryption and penetration testing (or other appropriate measures adopted) for storage of Oxford Brookes University data.
4.5	Appropriate auditing measures by the third party supplier must be in place to

	reduce the risk of compromise of the Oxford Brookes University data's confidentiality integrity and availability.
	SYSTEM ACQUISITION DEVELOPMENT AND MAINTENANCE
5.1	Procedures and policies and practice (to industry standard and as required by the University) must be in place to make sure that information security is an integral part of the contract or other arrangement.
5.2	The integrity, confidentiality and availability of any data must be maintained and appropriately protected when moving to a new solution or system or maintaining a system. All changes must be audited and documented.
	BUSINESS CONTINUITY MANAGEMENT AND SECURITY INCIDENT MANAGEMENT
6.1	The integrity confidentiality and availability of any data must be maintained and protected at the end of any contract or other arrangement or in the event of business interruption for whatever reason. Measures must be in place to ensure that security remains in place whatever the circumstance.
6.2	Physical controls and logical controls must be in place to ensure data security.
6.3	The third party supplier must be able to liaise with the University immediately to ensure that that normal business can be resumed as soon as practicable and any appropriate lessons can be learned from any break in security management.
6.4	There must be arrangements in place to ensure that any third party can be available for any subsequent investigation by any organisation or the Oxford Brookes University if appropriate. (Whether it is appropriate is to be decided by the Oxford Brookes University.)

APPENDIX 3

Below are some sample clauses which can be included in contracts to address information security and ensure compliance with UK data protection and privacy legislation. The clauses will need to be amended and numbered.

Particular care needs to be taken when identifying the roles: controller, processor or joint controllers of data. This matters because role dictates the contractual responsibilities. In the draft clauses, Party X is the data controller and Party Y is the data processor.

Definitions

Controller, Processor, Data Subject, Personal Data, Personal Data Breach, processing and appropriate technical and organisational measures: as defined in the Data Protection Legislation.

Data Protection Legislation: the UK Data Protection Legislation and any other European Union legislation relating to personal data, regulatory requirements, guidance and codes of practice.

UK Data Protection Legislation: all applicable data protection and privacy legislation in force in the UK including regulatory requirements guidance and codes of practice.

1. DATA PROTECTION

1.1 Both parties will comply with all applicable requirements of the Data Protection Legislation. This includes and is not restricted to providing details of Data Protection Officers and Privacy Policies.

1.2 The parties agree that for the purposes of the Data Protection Legislation, X is the Controller and the Y is the Processor. [Schedule [NUMBER] sets out the scope, nature and purpose of processing by the Provider, the duration of the processing and the types of Personal Data and categories of Data Subject.

1.3 X will ensure that the grounds for processing are identified and that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to Y [and/or lawful collection of the Personal Data by Y on behalf of X for the duration and purposes of this agreement.

1.4 Y shall:

a) process any Personal Data only on written instructions of X [which are set out in [Schedule [NUMBER]

b) ensure that it has in place appropriate technical and organisational measures, reviewed and approved by X to protect against unauthorised or unlawful processing of Personal Data

and against accidental loss or destruction of, or damage to, Personal Data The parties will have regard to the state of technological development and the cost of implementing any measures. Those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it;

c) ensure that all personnel who have access to and/or process Personal Data are suitably trained and are obliged to keep the Personal Data confidential; and

d) will not transfer any Personal Data outside of the European Economic Area unless the prior written consent of X has been obtained. Y will ensure the data subjects have enforceable rights and effective legal remedies; and that an adequate level of protection to any Personal Data that is transferred is provided and make this information available to X; and

e) will comply with all reasonable written instructions from Y

f) assist X , in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators; at no extra cost

g) notify X immediately on becoming aware of a Personal Data Breach;and to comply with subsequent legal and regulatory requirements and investigations promptly. To discuss the practicalities of addressing the consequences of the breacy with X, such as whether data subjects need to be notified.

h) at the written direction of X to delete or return Personal Data and copies thereof to the Customer on termination of the agreement unless required by Applicable Law to store the Personal Data; and

i) maintain complete and accurate records and information to demonstrate its compliance with this clause [NUMBER] [and allow for audits by X 's designated auditor and immediately inform X if, in the opinion of Y , an instruction infringes the Data Protection Legislation or if security is at risk;.

Either party may, at any time on not less than … **(15)** days' notice, revise this clause [NUMBER] by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when replaced by attachment to this agreement).

The Schedule (to be included in contracts in addition to the clauses above)

Processing; Personal Data and the Data Subjects

1. Processing by the Data Processor

    1.1 Scope of Processing

    1.2 Nature of Processing

    1.3 Purpose of the Processing

    1.4 Duration of the Processing

2. Types of Personal Data

3. Categories of Data Subject

APPENDIX 4

When engaging with third parties, as part of the procurement / information sharing :

1. Complete a Data Protection Privacy Impact Assessment (if required)

The Privacy Impact Assessment is used to determine the risk associated with processing data and whether or not mitigating controls will be sufficient. The guidance to help with completion of the assessment and the judgements to be making that decision can be found at:

> https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

If it is, the assessment is completed by the Faculty or Directorate with assistance from the IT Services Information Security team. The Privacy Impact Assessment must be retained and reviewed through the lifecycle of the agreement.

2. Complete an information risk assessment and risk treatment plan

Again these are completed by the Faculty / Directorate with assistance from the IT Services Information Security team. Any risks must be identified and minimised where possible and kept under review. The risk assessment and associated risk treatment plan must be kept by the Faculty or Directorate. This should inform how data can be shared, whether it can be minimised, if it can be encrypted etc.

3. Ensure security is part of the competitive tendering process

Where personal data or sensitive commercial data is involved the tender specification should consider information security and data protection requirements. This may be organisational security controls of the supplier (e.g. do they have a training programme, information security policies); technical controls of the desired solutions (e.g. does the solution encrypt data at rest and in transit, will be developed using secure coding practices, etc?). For guidance on the information security content of a competitive tender please contact the IT Services Information Security team.

4. Comply with procurement requirements

Any procurement requirements must be complied with. This includes finalising contractual arrangements.

5. Consider incorporating the contract clauses about data protection

See Appendix 3

6. Information Sharing Agreements

An information sharing agreement must be completed by the Faculty or Directorate in the absence of any contractual provisions about data protection and information security.

7. Signing the documents off

Any procurement paperwork, risk assessment contract or information sharing agreement need to be provide Legal Working Instruction Form to legal services for checking and signature.

8. Schedule reviews of the risk assessment and Privacy Impact Assessment as well as any contractual obligations

Ensure that they are regularly reviewed with a view to minimising security risk and to make sure that information is processed only when necessary.

9. Information security at contract termination

Consider what information security implications there are once a contract is due to be terminated. This may include revoking access permissions for third party supplier staff or systems, return of equipment or requesting the deletion or return of Brookes' data.