Data Security Guidelines for outsourcing and third party compliance

Contents

Introduction

This document contains guidelines that should be met to maintain the security of University information systems and data when the University enters into any arrangement with a third party.

Scope

This document should be understood by any member of the University who seeks to source a service from a third party that would give them direct access to University data. This may involve the service run on systems outside of the University in the cloud or where support agreements give the third party access to University systems.

Managing outsourcing risks

Prior to outsourcing or allowing third party access to the University's non-public information or systems, the risks involved must be clearly identified and documented. A review of the risks should be taken by at least one other person and senior member of staff should document that the risks identified are acceptable to the University. Advice from Procurement and the University Secretary's office should be sought during process

Formal outsourcing

Where a service is formally sourced a process must be contractually in place to ensure that information security standards are in place, maintained and reported on. A duty to report any breaches in security should be formally included in any contract and the frequency and timeliness of reports should be included within any contract.

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.

Appendix A contains a checklist of areas of data security that should be covered for during investigations of potential suppliers.

Contractual issues

All third parties who are given access to the University's non-public information or systems must agree to the following terms in any agreement;

- Compliance with the University's Electronic Information Systems Security Policy
- Compliance with the University's Data Protection Policy
- Appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier; and
- Confidentiality obligations where a third party is given access to the University`s non-public information
- Secure access routes and access rights required for maintenance based on the principal of least privilege
- Full auditing of all actions

Advice should be sought from the University Secretary's office and/or Procurement in relation to contractual issues and how these measures should be included. Use of third parties should not start until the University is satisfied that security measures are in place and a binding contract signed:

http://www.bath.ac.uk/procurement/

Personal Data

A Privacy Impact Assessment (PIA) is essential at the outset of any project that will potentially involve personal data being accessed by a third party. A comparison between a potential cloud service and an onsite service should be included if an onsite offering is available. 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 European Commission provides a list of countries [1] it has deemed to provide an adequate level of protection. Transfers to the USA can no longer be automatically approved following the ruling regarding the US EU Safe Harbour scheme. The ICO states that it may be possible to make transfers if Model Contract

[1] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
At time of writing -

Clauses [2] for the internal transfer of data are included in a contract - please contact Legal Services for advice in relation to any proposed agreement where data could be transferred to the USA.

Informal outsourcing

Commercial and free cloud providers offer convenience and simplicity for services such as email and storage. However, there are risks to their use and it is important that these are understood so that sensible decisions can be made about the suitability of their use for any given purpose.

Unlike formal outsourcing where the University negotiates the terms and conditions of a contract and carries out formal assessments and retains rights of intellectual property, users of the free services must accept the provider's terms and conditions. The University cannot ensure that confidentiality, integrity and availability of the information without a formal agreement in place. If there are legal or reputational consequences should the information you are storing be lost, stolen, or seen by unauthorised persons or organisations, you should not use a cloud service provider to store, transmit, or process it. 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.

Further guidance on cloud storage is published

http://www.bath.ac.uk/bucs/aboutbucs/policies-guidelines/cloud_storing_data_guidelines.html

Third party physical access

The University has secure areas where significant information assets are stored. Prior to a third party accessing these areas a risk assessment should be made taking including details of:

- Who the party is and the contractual arrangements
- What information systems the third party may have access to
- What information they could potentially access
- If supervision or monitoring is required
- If there are any other measures that could be taken to mitigate risk

Document Control Information

Owner	Mark Acres IT Security Manager
Version Number	0.01
Approval Date	
Approved By	
Date of Last review	

[2] https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf

Annex A

Cloud Services Provider Information Security and Privacy compliance tool

Date 8th June 2015

Version 0.21

Abstract

This document is designed to act as an aid to ensure that all areas of information security and privacy are included when checking a potential cloud service provider (CSP) for software as a service (SAAS)

Cloud Service Provider (CSP)

CSP Business Name	
Date of assessment	

Corporate identity of the CSP, processing role and contact information

CSP Registered company name	
CSP address and place of establishment	
Local representative in EU	
Data protection role in the relevant processing (controller, joint-controller, processor or sub-processor)	
Contact details for customer personal data protection related inquiries	
Contact details for Security related inquiries	

Data to be processed

Data owner within the University	
List of personal Data fields used	
Description of Restricted Data which may cause harm to the University if compromised	
Description of other data that will be stored	

Who will access data

List the roles in the University who would have access to data and their access rights	
List the roles of any members external to the University who may have access and under what circumstances	

CSP Policy and framework compliance

Please gives links to the Acceptable Use, Privacy and Security policies for the CSP.	
Please list any certifications or frameworks the CSP has or attests to.	

Ways in which data will be processed

Purpose that data will be processed	
Explicit contract indicating that data will not be processed in other ways or for other means by CSP other than for ensuring the service e.g. explicit that data not reused for marketing	
Explicit consent gathered from individuals	
How will University be informed about relevant changes to the service by the CSP	

Data storage and transfer

List data locations (including backups and failover service locations)	
Are any onward transfers made across boarders?	
Are all transfers encrypted (https/SSH)?	
Are subcontractors for any service e.g. backup?	
How will University be informed about relevant changes to subcontractors?	

Data Security Measures

Software / Client

Is any software required to be installed on University or client systems	

Update mechanisms for client software	
Any additional permissions or accounts required	

Physical / Data Centre / Personnel

Identify the physical precautions used to protect the data centre	
Identify the checks and precautions made on CSP staff	

Server / Cloud

Describe the processes and measures in place to manage the availability of the service such as backup Internet network links, redundant storage and effective data backup and restore mechanisms. Where possible describe the planned process to restore service in the event of catastrophic failure and expected timescales.	
Integrity: describe how the CSP ensures integrity (e.g., detecting alterations to personal data by cryptographic mechanisms such as message authentication codes or signatures). Where possible describe the greatest anticipated loss of data in the event of catastrophic failure.	
Describe how the CSP ensures confidentiality from a technical point of view (e.g., encryption of personal data 'in transit' and 'at rest' authorization mechanism and strong authentication). Where possible include what measures are taken to protect passwords when stored and retrieval mechanisms.	

Describe how the CSP ensures confidentiality from a from a contractual point of view, such as confidentiality agreements or confidentiality clauses, and company policies and procedures binding upon the CSP and any of its employees and subcontractors who may be able to access the data and assurance that only authorized persons can have access to data	
Describe how the CSP provides isolation (e.g., adequate governance of the rights and roles for accessing personal data (reviewed on a regular basis), access management based on least privilege principle, hardening of hypervisors (this is also relevant for the 'Integrity' section) and proper management of shared resources wherever virtual machines are used to share physical resources between different cloud customers	
Describe the update and patching mechanisms for operating systems and software to ensure that these are kept up to date	
Describe any vulnerability assessments made, their frequency and any policies in place to act on results	
Do any default passwords for the system exist?	
Describe how the CSP enables data subjects' rights of access, rectification, erasure, blocking and objection; in order to demonstrate the absence of technical and organizational obstacles to these requirements, including cases when data are further processed by subcontractors	

Monitoring

Detail the logs that the CSP states that they keep and monitoring and auditing on an ongoing basis	
Indicate the options that the University or independent certification authority has to monitor and or audit the logs in order to ensure that measures described in the contract are kept in an ongoing basis	

Data Portability, migration and transfer back assistance

Specify the formats, the preservation of logical relations, and any costs associated to portability of data, applications and services.	
Describe whether, how, and at what cost the CSP will assist customers in the possible migration of the data to another provider or back to an in-house IT environment	

Data retention, restitution and deletion

Describe the CSP's data retention policies and the conditions for returning the personal data and destroying the data once the service is terminated.	
Indicate for how long the personal data will or may be retained during the contract if an individual no longer makes use of the service	
Indicate for how long general data will or may be retained for.	
Indicate whether and how the cloud customer can request the CSP to comply with specific UK laws and regulations e.g. retain accounting	

material for 7 years if different standards apply in the location the CSP is situated	
Indicate the procedure for returning the individual personal data in a format allowing data portability	
Indicate the methods used to delete data, and whether data may be retained in backups after the cloud customer has deleted (or requested deletion of) the data, or after the termination of the contract, and in each case the period during which the CSP will retain the data	

Accountability and Transparency

Can the CSP enforce all relevant University of Bath policies? If no please state which policies cannot be enforced by the CSP	
Describe which technical, physical and organizational measures the CSP has in place to support transparency and to allow review by the customers for service provision	
Describe what policies/procedures the CSP has in place to ensure and demonstrate compliance by the CSP and its subcontractors or business associates, including by way of adoption of internal policies and mechanisms for ensuring such compliance. CSPs need to identify the elements that can be produced and provided as evidence to demonstrate norms' compliance and behaviour. CSPs need to identify the elements that can be produced and provided as evidence to demonstrate norms' compliance and behaviour. Evidence elements can take different	

forms, such as attestations, certifications, seals, third-party audits attestations, logs, audit trails, system maintenance records, or more general system reports and documentary evidence of all processing operations under its responsibility. These elements need to be provided at the • Organizational policies level to demonstrate that policies are correct and appropriate; • (ii) IT Controls level, to demonstrate that appropriate controls have been deployed; at • (iii) Operations level, to demonstrate that systems are behaving (or not) as planned. Examples of evidence elements pertaining to the different levels are privacy seals (i), Certifications like CSA Certification -OCF Level 2 (ii) and logs (iii) produced by reliable monitoring and comprehensive logging mechanism, (iv) audit trails	

Security Incident and Personal Data Breach notification

Specify how the CSP defines a security incident and personal data breach	
Specify how the customer will be informed of personal data and data security breaches affecting the customer's data processed by the CSP and/or its subcontractors, within what timeframe and how	

Cooperation

Specify how the CSP will co-operate with the University of Bath in order to ensure compliance with applicable data protection provisions: e.g., to enable the customer to effectively guarantee the exercise of data subjects' rights (right of access, correction, erasure, blocking, opposition), to manage incidents including forensic analysis in case of security breach.	
Describe how the CSP will make the information necessary to demonstrate compliance available to the customer and supervisory authorities	

Legally required disclosure

Describe the process in place to manage and respond to requests for disclosure of personal data by Law Enforcement Authorities; with special attention to notification procedures to interested customers, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation	

Business continuity and data loss

Is the data business critical?	
Can the data be retrieved in the event that the CSP closes or goes out of business?	
Do the CSP SLA for availability meet University requirements?	
Do the SLA compensation plans adequately compensate for actual damage caused by a loss	

of service or data – the damage done to University or service reputation may not be repaired by receiving a token amount of free service	

References

Cloud Security Alliance

"Privacy Level Agreement [V2]: A Compliance Tool for Providing Cloud Services in the European Union"

https://downloads.cloudsecurityalliance.org/assets/research/pla/downloads/2015_05_28_PrivacyLevelAgreementV2_FINAL_JRS5.pdf

"Cloud Controls Matrix (CCM)"

https://cloudsecurityalliance.org/research/ccm/#downloads

European Union Agency for Network and Information Security –

Cloud Computing Risk assessment

https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

Jisc Legal

Cloud Computing Contracts, SLAs and Terms & Conditions of Use

http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2141/User-Guide-Cloud-Computing-Contracts-SLAs-and-Terms-Conditions-of-Use-31082011.aspx

Security Frameworks and Certifications

- AICPA 2014 Trust Services Criteria (SAS70, SSAE 16 SOC[1,2,3])
- COBIT 5.0
- CSA Enterprise Architecture
- CSA Security, Trust and Assurance Registry (STAR)
- ENISA (European Network Information and Security Agency) Information Assurance Framework
- European Union Data Protection Directive 95/36/EC
- ISO/IEC 27001:2013
- NIST SP800-53 Rev 3 Appendix J
- ODCA (Open Data Center Alliance) Usage Model PAAS Interoperability Rev. 2.0
- PCI DSS v3

Amendment History

Version	Date	Author	Summary
0.1	20150109	Mark Acres	First draft based on Australian Government Department of Defence requirements http://www.asd.gov.au/publications/protect/cloud_computing_security_considerations.htm
0.2	20150606	Mark Acres	Completely revised draft to include EU privacy requirements https://downloads.cloudsecurityalliance.org/assets/research/pla/downloads/2015_05_28_PrivacyLevelAgreementV2_FINAL_JRS5.pdf
0.21	20150608	Mark Acres	Correction and additional fields for clarity