Loughborough University

Information Security

Information Service and Service Contractors Policy

Version 1.0:
Approved June 2016
Review June 2020

Information Service and Service Contractors Policy

1. Policy Overview

To provide some elements of its IT infrastructure and corporate and local IT systems cost effectively, the University works with a range of external partners. For example, IT solutions may be hosted by systems operated by the partner, information systems such as Agresso and iTrent are supported under contract with the company which develop and maintains them. Also remote monitoring services may be purchased from a partner organisation. As part of the contracts relating to these services, third party organisations are likely to require physical and/or remote access to University information and systems.

To ensure the security and integrity of University information and systems, this policy sets out the conditions for providing access to third party organisations in the contractual context outlined above. It should be read in conjunction with the Management of User Access to Information policy which covers authorization of individual access to information and systems.

2. Policy Audience

The majority of this policy applies to IT Services and Facilities Management staff. Schools and other Professional Services within the University should also use this policy when procuring services which require providing access to locally managed information or physical and/or remote access to locally managed infrastructure, information or systems.

This policy applies to:

- Service Providers – These are external to the University, and may maintain systems on the University's behalf. Service Providers are likely to require remote access to University information systems.
- Service Contractors – These are external to the University, and may host systems externally on behalf of the University. Service Contractors are likely to require access to University information to provide a service.

This policy should be referenced:

- When third party organisations are involved in the design, development or operation of information systems for the University. There may be many reasons for this to happen, including installing and configuring commercially developed software, third party maintenance or operation of systems, to full outsourcing of an IT facility. (Service Provider)
- When 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. (Service Provider)

- When users who are not members of the University are given access to information or information systems. (Service Provider)
- When a service is outsourced to a third party which involves University data being hosted at an external location outside the control of the University. (Service Contractor)

3. Policy Sections

The policy section has been separated depending on the type of service.

4. Service Provider

Staff responsible for agreeing service, maintenance and support contracts will ensure that the contracts being signed are in accordance with the University's Information Governance Policies. This will require review of the relevant policies and procedural documentation of the partner organisation.

Service owners/managers must assess the risk to the information and services to be covered by the contract. If Confidential information is to be shared the service provider will be required to sign a confidentiality agreement. Access to Highly Confidential information will not be given to service providers unless the arrangement is part of the initial contractual arrangements relating to the information. Should any changes be required subsequently, the authorization of all relevant parties must be obtained and documented in advance of any changes to previously agreed arrangements for ensuring the security of the Highly Confidential information.

If a service is being procured which requires that a third party has enhanced access to critical University infrastructure, the contractual terms must be approved and signed by the Chief Operating Officer before implementation of the service.

Physical access to locations which are deemed high value security risk areas (e.g. locations containing core networking equipment) must be arranged in advance and service providers must be accompanied in these locations at all times by a member of University Security, Facilities Management or IT Services personnel.

Where remote access to information systems is required, the Remote Access to Server(s) Procedure needs to be followed by the service provider conducting the work. The following information will be required:

- Remote IP address which will be used to connect to the University's information systems;
- Primary contact in the organisation, including name, job title, telephone number and email address.

The form can be found at:

www.lboro.ac.uk/services/registry/information-governance/policy5/

Completed forms should be forwarded to the IT Service Desk.

Prior to the service provider conducting any work, a detailed change request must be completed. Only if the request is approved under the IT Services Change Management Process will access be granted.

Standard user accounts (-remote accounts), which have no administrative privileges, will be provided to service provider staff to allow access under the Management of User Access to Information policy. Only protocols approved by IT Services will be authorised for use and usage will be monitored and logs retained as per the data retention period.

Staff responsible for agreeing and approving changes must ensure that all changes made are logged for auditing requirements.

5. Service Contractor

Staff responsible for agreeing service, maintenance and support contracts will ensure that the contracts being signed are in accordance with the University's Information Governance Policies. This will require review of the relevant policies and procedural documentation of the partner organisation.

Service owners/managers must assess the risk to the information and services to be covered by the contract. If Confidential information is to be shared the service provider will be required to sign a confidentiality agreement. Access to Highly Confidential information will not be given to service providers unless the arrangement is part of the initial contractual arrangements relating to the information. Should any changes be required subsequently, the authorization of all relevant parties must be obtained and documented in advance of any changes to previously agreed arrangements for ensuring the security of the Highly Confidential information.

When transferring data to the Service Contractor, unless the information falls into the Public or Not Sensitive information category, the transfer should be conducted via a secure means (encrypting the data first).

Prior to procuring external hosted services, where relevant detailed information should be obtained from the external contractor and reviewed by IT Services. This is to ensure that the contractor is capable of handling the University's information securely. Examples of the type of information required can be found in Appendix A.

Appendix A: Example questions for External Contractors

- Is the service contractor ISO27001 certified?
  This certification formally specifies a management system that is intended to bring information security under explicit management control.
- Can the service contractor provide a copy of their information security policy?
  This policy would outline the management controls that are in place to manage information security.
- Can the service contractor provide a copy of their data retention policy?
  This would indicate the length of time the contractor would hold the University's information.
- Is the service contractor on the Data Protection register?
  Every organization that processes personal information must notify the Information Commissioner's Office. This information is then held in the form of the Data Protection Register.
- If the service contractor is going to be processing electronic payments on behalf of the University, are they PCI DSS compliant?
  PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This standard is intended to help organisations proactively protect user account data.
- Is the service contractor subject to regular security testing (penetration testing) or Information Security audit?
  This is to ensure that service contractors, which are certified against any information security standards, are still compliant. Penetration testing will ensure that the contractors' infrastructure is secure.
- Can the service contractor ensure that all web applications, which leverage the University information will be conducted via secure web (HTTPS)?
  This is to ensure that if Confidential information is involved in the service provision it is communicated securely.
- Does the contract include appropriate Data Protection assurances in-line with EU Data Protection equivalency requirements? As controls change frequently, please contact the IT Service Desk for advice.