IT Security for 3rd Parties, Suppliers and Support Organisations Policy

Version Control

Version	Date
Draft 0.1	28/09/2017
1.0	01/11/2017

Related Polices

- Information Services Acceptable Use Policy
- Associate Accounts Policy
- Data Storage and Remote Working Policy
- Password Usage and Management Policy
- Access Control Policy

1. Introduction

This policy sets out the conditions that are required to maintain the security of the University's information and IT systems when third parties, other than the university's own staff or students or systems, are involved in their operation. There are 4 possible circumstances when this may occur:

- When 3rd parties (for example contractors/suppliers) are involved in the design, development or operation of university information systems or IT equipment.
- When access is granted to 3rd parties from locations outside of the university network and equipment may not be under the control of the university.
- The use of cloud computing services.

2. Scope

This document applies to any member of the university who is considering engaging a third party to supply a service where that service may require access to the university's information assets and includes statements on:

- Informal outsourcing
- Managing outsourcing and third-party access risks.
- Contractual Issues.
- Third Party support and maintenance.
- Facilities Management and Outsourcing.
- Physical Access by External Parties to Sensitive Areas.
- Electronic Remote Access by External Parties

3. Informal Outsourcing

Staff and students at the university are able to access and use a range of IT services on the Internet which are provided by third parties with which the University has no formal agreement. Informal Outsourcing services must not be used for storage or transmission of any university data. Staff should contact IT Services before using any such service so it can be assessed and approved. Examples of informal outsourcing include:

- Dropbox, Google Drive, Gmail, Hotmail, Survey Monkey or similar services

- Internet / ‘Cloud’ based services used for any storage, processing or transmission of University data of any kind

3.1. Risks of Informal Outsourcing

Due to the absence of controls or accountability to the university, a number of security risks are associated with entrusting information to these facilities. Some of the potential risks are listed below:

- Who has access to the information?
- How the information is used.
- Where the information is stored.
- How securely the information is stored.
- Will the data be lost in the event of a disaster?
- Use of these facilities to process data may be in breach of the Data Protection Act 1998 and GDPR legislation.

With the risks highlighted in above, wherever possible, University staff should only use services provided by the University for conducting University business. Where a University solution is not provided, however, then staff may use third party systems but must not store or transfer out of the University the following types of information:

- Confidential Information – business confidential information (which may or may not also be personal information) and which may not be disclosed except to those with the explicit consent of the data owners and where disclosure may constitute an actionable offence.
- Sensitive Personal Information – information covered by the Data Protection Act 1998 which relates to an individual’s ethnicity, political membership or opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, the commission or alleged commission of an offence and any related proceedings.
- Personal Information – information covered by the Data Protection Act 1998 that allows a living individual to be identified or which relates to an identifiable individual.

4. Access Control for 3rd Parties

Third party access to systems must be restricted to the minimum required system level access.

Any 3rd party companies and personnel requiring access to University IT systems and data must show written agreement to follow established procedures governed by existing policies:

- Information Services Acceptable Use Policy
- Access Control Policy
- Password Usage and Management Policy
- Mobile and Remote Working Policy
- Associate Accounts Policy

4.1. Contractual Issues

All third parties given access to the university's IT systems must agree to abide by the University's IT security policies prior to being granted access.

The university will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the University will require third party suppliers of services to sign a confidentiality agreement to protect its information assets.

Where relevant, third parties will be asked to provide a copy of their information security policies.

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.

4.2. Commissioning of New Services by 3rd Parties

Any new services commissioned by 3rd Parties must adhere to the IT security policies as part of the commissioning process. In particular:

- Access Control Policy

- Password Usage and Management Policy

University staff responsible for procurement of any service or system that connects to the University's IT infrastructure in anyway and any contracts for maintenance and support for such system will ensure that contracts being signed are in accordance with the all of the University's IT Security Policies. Contracts should be approved with IT Services and any relevant committees such as the IT Programme Board prior to signing or commitment to purchase

5. Physical Access by External Parties to Sensitive Areas

A risk assessment must be made by the initiator in collaboration with a member of the 3rd line IT Support Team and appropriate controls established before granting third party access to secure areas where confidential information is stored or processed. This also applies to secure areas containing active network equipment.