1. Introduction

1.1. This information security policy document sets out principles and expectations about maintaining the security of University IT facilities that are accessed, or provided by third parties. It is a sub-document of Information Security Policy (ISP-S1).

1.2. Definitions:

- Third parties – external organisations, or individuals other than the University’s own staff or students.
- Confidential information - information which if improperly disclosed or lost could cause harm or distress to individuals, or financial loss or reputational damage to the University. This includes personal data, as defined by the Data Protection Act, and other valuable or sensitive information not in the public domain, such as information that is commercially confidential for the University or a third party, and information related to intellectual property.

1.3. This document includes statements on:

- Formally provided, and informally available, IT facilities and services
- Managing outsourcing and third party access risks
- Contractual issues
- Third party support, maintenance and development
- Guest access by third parties
- Physical access by external parties to sensitive areas

2. Formally provided, and informally available, IT facilities and services

2.1. Formally provided University IT facilities and services are those:

- Either provided directly by University departments and managed by University staff
- Or provided to the University by third parties and subject either to formal bilateral agreement or clear understandings setting out standards and expectations which cover information security.

2.2. Informally available IT facilities (informal outsourcing):

- Staff and students are able to access and use a range of IT facilities on the Internet which are provided by third parties with which the University does not have any formal agreement or established understanding. Users signing up to use these facilities are typically required to accept the terms and conditions of a unilateral agreement entirely determined by the provider.

- Examples of informal IT outsourcing include:
Using Google Docs for University business \textit{(with no formal bilateral agreement)}.

Using MSN Hotmail or Google Mail for University business \textit{(with no formal bilateral agreement)}.

Forwarding University business email from a University email account to MSN Hotmail or Google Mail \textit{(with no formal bilateral agreement)}.

- In the absence of any control by or accountability to the University, a number of possible security risks are associated with entrusting information to these facilities. The potential risks include a lack of knowledge and control over:
  - Who may have access to user data
  - How user data is used
  - Where user data is stored
  - How securely user data is stored
  - How reliable and available the facility will be in the short term
  - How viable the facility will be in the long term
  - How the facility may change in terms of user interface or nature of service
  - Whether user data will be recovered in the event of a disaster
  - How much support will be provided in the event of a problem

- Use of informally outsourced IT arrangements to process personal data may range from being inadvisable to breaching aspects of the Data Protection Act.

- Given the risks above, such facilities must not be used, or depended upon, for working with confidential University information or for processing the personal data of third parties.

- Staff who demonstrate informally outsourced IT facilities must not promote or approve their use for handling confidential information (and preferably should also warn against such use).

- Staff must not configure their University email accounts to automatically forward incoming email to services that are not operated by the University, unless such an arrangement has been formally approved by the Director of IT Services and is subject to an appropriate bilateral contract.

3. Managing outsourcing and third party access risks

3.1. Staff of sufficient seniority must be involved in, and take responsibility for, ensuring that risks are identified and managed where University IT systems are to be accessed, or provided, by third party individuals or organisations, and that such solutions are compatible with the University’s broader IT strategy. The purpose is to protect the interests of the University, its members and to ensure legal compliance.

3.2. IT Services must in the first instance be consulted to determine whether the IT facility or service is compatible with the University’s broader IT strategy.

3.3. Where the IT facility or service is not compatible with the University’s broader IT strategy either an alternative solution must be found or approval to proceed must be obtained from the PVC (IT) or the Registrar & Secretary as appropriate who will take into account the concerns raised by IT Services.
3.4. A risk assessment must be used to help decide:
- Whether the IT facility or service is an acceptable solution from both a systems design and a technical perspective;
- Whether the IT facility or service is an acceptable solution from an information security perspective;
- Whether a formal agreement with the third party is needed and if so what it should include. (See also “contractual issues” below.)

3.5. The risk assessment must be undertaken in conjunction with staff from IT Services and from Information Assurance Services.

3.6. The risk assessment, which in some cases may conclude that an activity cannot safely proceed, must include:
- General analysis of the proposed arrangement in terms of its acceptability from both a systems design and a technical perspective.
- General analysis of the proposed arrangement in terms of any new or increased information security risks. In particular, consideration of what University information will become accessible to the third party organisation. In doing so potential legal compliance risks are to be identified, e.g. relating to Data Protection legislation.
- Determination of whether the third party is already subject to an agreement with the University e.g. is providing a service that has been purchased subject to standard University terms and conditions.
- An assessment of the potential impact on University business that could result from the third party suffering or causing a problem i.e. understand potential risk impact in terms of scope and severity.
- An assessment of how trustworthy and competent the third party is in relation to undertaking the proposed arrangement or activity.

3.7. Where the risk assessment concludes that an activity cannot safely proceed either an alternative solution must be found or approval to proceed must be obtained from the PVC (IT) or the Registrar & Secretary as appropriate who will take into account the conclusions of the risk assessment.

4. Contractual issues

4.1. Where it is determined that a formal agreement is to be made with a third party in relation to accessing or providing University IT facilities, the following issues must be addressed:
- The third party must agree to follow University information security policies. The information security policies, or a summary, must be formally provided to any such third party prior to their being granted access.
- Where relevant, third parties should be asked to provide a copy of their information security policies. Enquiries should be made in writing relating to any concerns arising.
- All orders/contracts for the provision of services should be issued on the basis that the University’s standard terms and conditions of contract shall apply. These include standard clauses on confidentiality and data protection. Where an
agreement is being negotiated separately then these two standard clauses should be included in that agreement. Where this is not possible then advice should be sought from Information Assurance Services prior to any agreement being concluded. The University’s Procurement Regulations also stipulate that the IT Category Manager must approve the use of any contract conditions where they are not the University’s standard terms and conditions.

- Any specific arrangements that may be required by the University in relation to assuring information security must be negotiated and included in the agreement. For example, any specific responsibilities, security controls, monitoring or reporting that may be required.

- The potential effects of termination of the agreement, or its transfer/assignment to another organisation, must be considered and controlled if possible. Matters relating to ongoing security of University information in the event of contract termination should be taken into account. If there is to be a handover of a service between two third parties, there should not be a period when neither or both parties may be considered to have responsibility for, or control of, the service.

- Where appropriate binding service level agreements should be negotiated that specify the performance to be delivered and the remedies in case of non-compliance.

- It is highly advisable to agree the details of liability clauses up front.

- The contract and any associated service level agreement should be subject to formal review by the Purchasing Office, IT Services and Information Assurance Services, and additionally by the University’s legal advisers where this is considered necessary.

5. Guest access by third parties

5.1. Where third parties are involved in providing support and maintenance of University IT facilities it may be necessary for them to access systems using the highest levels of privilege. It is essential in that:

- Such privileged access by third parties to, or via, the University network is in all cases approved by and where necessary facilitated by IT Services.

- A member of University staff is responsible for managing the access provided in terms of scope, level and duration. It is also recommended that third party access is monitored or logged.

- Privileged remote access arrangements must only be permitted via secure encrypted network protocols. See also Cryptography Policy (ISP-S16).

- The third party has provided the University with the code of practice that their staff and agents must follow in handling customer’s information. The code of practice provided by the third party has been reviewed, is acceptable and the University has assurance in writing that the code will be followed. It is preferable that this forms part of the agreement with the third party for provision of the service.

5.2. Where third parties are to be involved in the provision of bespoke University information systems or software it is essential that:

- The third party can provide credible assurances of security quality controls or standards in relation to their applications development process.
• Use of the application as an element of the University’s production systems is not permitted if it is known to have serious security vulnerability. See also Software Management Policy (ISP-S13).

5.3. Changes, by a third party organisation to a University information system, must be subject to the same change management procedure that would apply if those changes were being made by University staff.

6. Third party support, maintenance and development

6.1. University members must not permit information security safeguards and policies to be bypassed, or allow inappropriate levels of access to University information or IT facilities to other members or any third parties such as guests, customers, collaborators, suppliers, consultants or contractors. See also Use of Computers Policy (ISP-S9).

6.2. Any access to University information systems provided to third parties must follow established recognised procedures. For example procedures are currently available for providing guests and conference delegates with temporary central service user accounts or wireless Internet access. See also User Management Policy (ISP-S8).

7. Physical access by external parties to sensitive areas

7.1. A risk assessment must be made and appropriate controls established before external parties, such as contractors, are given access to normally secure areas where confidential information is stored or processed. This is likely to apply particularly to computer machine rooms and certain offices. The potential risks include:

- Disclosure or theft of confidential information
- Theft or tampering with equipment
- Accidental damage to equipment
- Misuse of facilities

The outcome of the risk assessment may be to deny access, simply grant access or provide access whilst taking steps to manage the risks. For example, access may need to be supervised, or it may be that sensitive information or equipment is first removed or given additional protection. See also Building Security (ISP-I1).

| Failure to comply with University Policy may lead to disciplinary action. |

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.