## GISP22. Working with third parties

| | |
|---|---|
| Date: | 5 October 2017 |
| Version: | 2.0 |
| Authors: | Raymond Scott |
| Quality Assurance: | Information Strategy and Services Committee (ISSC) |

### *Version control*

| Revision | Date | Revision Description |
|---|---|---|
| 1.0 | 8/11/12 | Approved by ISSC |
| 1.1 | 5/10/17 | Reviewed and updated |
| 2.0 | 20/10/17 | Approved by ISSC |

### *Policy*

| | |
|---|---|
| Security Control | Controls to maintain security of the University's information and systems when third parties, i.e. those other than University staff or students, are involved in their operation. |
| Objective | To ensure that information security is considered and risks minimised when the University works with contractors involved in the design, development or operation of information systems, or when users who are not members of the University are given access to information or information systems. |
| Policy | 22.1. All contracts with external suppliers for the supply of services to the organisation must be monitored and reviewed annually 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 and must be complete with contact details of all personnel concerned.<br>22.2. Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the contents and spirit of the organisation's information security policies.<br>22.3. Persons responsible for commissioning outsourced development of computer based systems and services must exercise due diligence and use reputable companies that operate in accordance with quality standards and which will follow the information security policies of this organisation, in particular those relating to application development.<br>22.4. Where responsibility for maintaining security standards is shared between the external supplier and the University, the agreement shall detail where the responsibility lies (with the supplier or the University). |

| | |
|---|---|
| | 22.5. All external suppliers who are contracted to supply services to the organisation must agree to follow the information security policies of the organisation. An appropriate summary of the information security policies must be formally delivered to any such supplier, prior to any supply of services.<br>22.6. Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is important.<br>22.7. An appropriate summary of the information security policies must be formally delivered to any contractor, prior to any supply of services.<br>22.8. An appropriate summary of the information security policies must be formally delivered to, and accepted by, all temporary staff, prior to their starting any work for the organisation.<br>22.9. Any facilities management, outsourcing or similar company with which this organisation may do business must be able to demonstrate compliance with this organisation's information security policies and enter in to binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance. |
| Responsibility | • Data and system owners will assess the risk to its information posed by providing third party access before granting access. Where necessary, data and system owners will require third parties to sign confidentiality agreements to protect the information assets.<br>• ITCS is responsible for ensuring that service or support and maintenance agreements with third parties are in accord with the University's information security policies.<br>• Third parties are responsible for ensuring their computer systems are safe, secure and operated within legal frameworks and used in accordance with this security policy and the Conditions of Computer Use.<br>• All third parties given access to University information systems must agree to follow the University information security policies. |
| Incident Management | Incidents should be reported to the IT Service Desk in the first instance for investigation by the Strategy, Policy and Compliance team as described in GISP14. |