Third Party Information Security Governance

Andrew Meikle February 2018

1 Introduction

This document identifies roles and responsibilities within the university for:

- Ensuring that the appropriate contractual obligations are put in place
- Determining whether a Data Protection Impact Assessment (DPIA) is required
- Writing and agreeing a DPIA when required
- Determining the basis on which subject data is held in the system
- Identifying and testing the security controls that the supplier has in place

It also describes the process by which existing suppliers will be reassessed and the process by which the university will respond to future changes in legislation

2 Roles, Responsibilities and Accountabilities

2.1 Contractual Obligations

Information Systems Services (ISS), Strategic Governance and Planning (SPG) and Procurement have agreed a set of data protection contractual obligations to be put in place for existing and future contracts with software or software service suppliers.

Awareness raising regarding information security and data protection is led via SPG working in partnership with ISS to ensure that staff procuring software are aware of the need for appropriate controls for 3rd party software. Enquiries on details can will be managed through the Head of Corporate Information Systems (CIS).

New contracts with such suppliers are identified through the procurement process to ensure that new suppliers have appropriate contracts. An extra process is triggered when procurements are coded against software purchases to ensure that the Head of CIS can determine the appropriate obligations on both the university and the software/service supplier.

2.2 Requirement for Data Protection Impact Assessment

The Head of CIS, in consultation with SPG will determine whether data to be held in the software/service requires protection under the GDPR.

2.3 Agreeing a Data Protection Impact Assessment

If it is determined that a DPIA must be in place, then that will be drafted jointly by the Head of CIS or their delegate and SPG. That DPIA will become part of the binding contract between the University and the Supplier.

2.4 Security Controls

Suppliers will be required to indicate the technical and human controls that they have in place to protect university data and the regime they use to ensure the fidelity of those controls.

For example, Data held in an EU data centre would be expected to have controls at least equivalent to ISO 27001; we would expect to be provided with the scope, definition and results of a recent external penetration test and a schedule for the resolution of any issues identified through that testing.

The IT Security Manager is responsible for determining whether the supplier's controls are sufficient to the university's requirements.

3 Reassessment of Suppliers

The Head of CIS in conjunction with the IT Security Manager will periodically determine whether changes to suppliers' software/service warrants:

1. A reassessment of the Information Security controls provided by the supplier
2. An update to the Data Protection Impact Assessment
3. An update to any subject facing documentation explaining the university's holding of data in the system

4 Future Legislative Changes

SPG are responsible for notifying departments and divisions of changes to legislation relating to Data Protection. Where this occurs, this document and the responsibilities it lays out will be reviewed and updated.