Information Services

Birkbeck Information Security Policy

Supporting Policy 9: Birkbeck Supplier Relationship Policy

Approved by Strategic Planning Committee

15 September 2022

0. Context

This policy forms part of the Birkbeck IT Regulations.

1. Introduction

Arrangements involving third party access to/ supply of Birkbeck's computer systems must be set out in a formal contract to ensure compliance with the College's general policies on information security and the associated codes of practice.

2. Purpose

The purpose of this policy is to ensure protection of the College's assets when they are accessible by the supplier and that this protection is documented and that any activity carried out on behalf of the College by third parties is controlled and managed by the College. Any individuals carrying out work must be made aware of this policy and the context within which it stands - the Birkbeck IT Regulations.

3. Scope

This policy applies to all third parties given access to College information systems and College staff entering into any such arrangements – whether that is for supply of IT systems/software or access to/management of these.

4. Requirements

4.1 A **risk assessment** shall be carried out before entering into a contract with any supplier. Potential risks, particularly involving small companies, include non-performance, delays in attending on site, expertise being invested in a single person and under resourcing, for example, owing to other contractual obligations.

4.2 Any contract or agreement should be drawn up by Birkbeck, rather than the supplier. Where this is not possible, then at the very least, the contract shall require acceptance of Birkbeck Terms and Conditions and the Birkbeck IT Regulations by the supplier.

4.3 Birkbeck staff entering into any arrangements must be aware of any obligations on them or the College and must be authorised to sign the contract on behalf of the College. It is particularly important to reach agreement on public liability insurance and damage liability.

4.4 The contract should list target timescales, agree how evidence of work completed to schedule will be presented and specify payment penalties if schedules are not met.

4.5 The contract must be in place **before** access to any system is provided and a copy of the relevant policies and codes of practice provided to the vendor/supplier. Anyone with access to Birkbeck systems is bound by the Birkbeck IT Regulations.

4.6 Depending on what is being contracted for, there will be different requirements for the supplier to adhere to. For example, for outsourced IT service management, see Supporting Policy xx: Birkbeck Outsourced IT Service Management Policy. For web presences, see Supporting Policy xx: Birkbeck Web Presence Policy.

4.7 Supplier requirements include technical controls, and these necessarily change when technological capabilities change. This policy requires that associated codes of practice identified in policy documents are followed (codes of practice will be approved by the IT Security and Governance Group).

The following items should be considered/checked for inclusion in the contract:

a. A description of each computer system to be made available to the contractor;
b. A requirement to maintain a list of individuals authorised to use the contracted service;
c. The times and dates when the contracted service is to be available;
d. The respective obligations, responsibilities and liabilities of the parties to the agreement;
e. Procedures regarding the protection of Birkbeck's assets, intellectual property rights and the confidentiality of the information contained therein;
f. Restrictions on the copying and disclosure of information;
g. Responsibilities to comply with the current UK/EU legislation and Birkbeck policies;
h. Conditions determining the right of access to the JANET network;
i. The right of Birkbeck to monitor and revoke user activity;

j. Measures to ensure the return or destruction of information and assets at the end of the contract; contractors must guarantee to erase all disks, tapes and other media returned to them (for example under warranty or field service exchange). Contractors must indemnify Birkbeck against any liability arising from any failure of their data erasure procedures.
k. Responsibilities regarding hardware and software installation, maintenance and protection which must include a commitment to implement best-practice security procedures;
l. Involvement by the third party with sub-contractors and other participants.

Data Protection Act 2018

Note also the responsibilities of contractors and other third parties in relation to the processing of personal information on behalf of Birkbeck, as set out in Birkbeck's Data Protection Policy.