Birkbeck
UNIVERSITY OF LONDON

Information Services

Birkbeck Information Security Policy

Code of Practice 4 – Network Connections

Approved by: ITSAG

10 May 2023

1. Context

This code of practice forms part of the Birkbeck IT Regulations and must be read and understood in that context. For more information, contact Birkbeck IT Services, a link to their contact details is available on the Birkbeck IT Regulations page.

2. Introduction

The purpose of this code of practice is to set out the procedures for connecting equipment to the Birkbeck network.

This code of practice is designed to minimise the potential exposure to the College from risks associated with connected equipment.

This code of practice applies to anybody connecting to the Birkbeck network whether wired or wireless access.

Requests to allow access to the College's network must meet the following criteria.

3. Records

3.1 Any IT system that is out of vendor support for firmware/operating system/software but has been allowed by Birkbeck Information Security or the CIO to be connected to the network must be recorded by ITS and that item will be kept with the risk register.

4. Connecting equipment

4.1 When connecting equipment/services, owners of systems will need to register names of (new) hosts with ITS and provide appropriate information:

- Name of the host
- IP address(es) of the host
- Owner/user of the application(s) on the host
- What services are provided by the host both internally and, more importantly, to the public
- Maintainer of the host
- Expected lifetime of the host/application/service.

ITS will record and manage these records and keep DNS records accurate (both forward and reverse). ITS will also regularly review the records for accuracy/relevance (hence 'expected lifetime' request above).

4.2 Any new user-facing services must be protected by multi-factor authentication using the College's Azure AD.

4.3 Any service that is to be visible outside the College must be in the DMZ and employ proxies. Both the DMZ and the proxies used must be approved by Birkbeck Information Security.

5. Decommissioning equipment

5.1 When equipment is being decommissioned, there are certain housekeeping actions which must be carried out by whoever is decommissioning. These include, but are not limited to, removing the relevant records in the DNS and removing any rules on the firewalls.