Birkbeck
UNIVERSITY OF LONDON

Information Services

Birkbeck Information Security Policy

Supporting Policy 11: Birkbeck Network Connection Policy

Approved by Strategic Planning Committee

1 March 2023

0. Context

This policy forms part of the Birkbeck IT Regulations. For more information, contact Birkbeck IT Services, a link to their contact details is available on the Birkbeck IT Regulations page.

1. Introduction

The Birkbeck network, and the systems connected to it, are critical to the administrative, teaching and learning and research activities of the College. Responsibilities for the network lie both with those administering them and with the users of the network.

2. Purpose

The purpose of this policy is to:

- ensure that the College's IT network and computing facilities are adequately protected against misuse or abuse;
- create awareness of the need to safeguard the effective operation of the IT network by implementing appropriate security measures;
- ensure all system administrators and network users understand their own responsibilities for protecting the network;
- ensure the high availability and effectiveness of the network and facilitate fast resolution of any problems by ITS and others;
- protect Birkbeck's reputation;
- help preserve the integrity and privacy of users' data; and
- reduce interruptions to the service (and unnecessary support calls).

3. Scope and definitions

This policy will cover all equipment, irrespective of ownership, attached to the College network, whether directly through wired connections, or using wireless technologies, or by making virtual connections using a virtual private network (VPN) and their use within the Birkbeck Acceptable Use Policy.
An IP address is deemed to include both IPv4 and IPv6 addresses.
Attachment is defined as either:

- connection to the College network that results in the device being allocated an IP address belonging to, or managed by, Birkbeck (this will include devices connected using a VPN terminating within Birkbeck or using eduroam within the College) or
- connection at layer 2.

The College network comprises network hardware (e.g. routers, switches, wireless access points) owned or managed by Birkbeck ITS.

4. Responsibilities for all network users

4.1 New connections of equipment to the College network may only be made with the authority of Birkbeck Information Security or the CIO. Process for request/notification is in the Code of Practice. Users are permitted to plug in client machines, but not extend the network in any way.

4.2 Users must not provide Wifi networks within the Birkbeck campus except with **prior approval** from Birkbeck Information Security or the CIO.

4.3 Access to the College network must not be shared with unauthorised users.

4.4 Connected equipment must be maintained in accordance with manufacturers' recommendations. Operating system and application software must be kept up to date to ensure risk from security vulnerabilities is minimised. Equipment must not be, or remain, connected to the network after a manufacturer ceases to provide security patches without the **prior approval** of Birkbeck Information Security or the CIO.

5. Management of the network

5.1 The College's network shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity in collaboration with individual system owners. Where network infrastructure is not managed by ITS, read-only access to devices must be provided to ITS for the purpose of ITS being able to monitor the entire network. All network management staff shall be given relevant training in information security issues.

5.2 Any staff creating services must register all IP addresses in line with the Code of Practice (who will create an appropriate entry in the Domain Name System) and this registration must be kept up to date.

5.3 Appropriate logs must be kept so that it is always possible to determine who/what was using a particular IP address at a particular time. Logs shall be retained for as long as is necessary, kept securely and a record kept of how long each set of logs is kept.

5.4 Machines must be disconnected from the network when requested by ITS. Such requests are typically made when a system has caused problems to other users of the network or to an external network and/or following a security breach. Systems must **not** be reconnected to the network without the explicit authorisation of the Birkbeck Information Security Team or the CIO.

5.5 The protocols currently allowed for routing on the Birkbeck network are those comprising the Internet Protocol suite. Any other protocols must be approved by ITS.

5.6 In the event of unacceptable network events occurring on a local network, or in order to safeguard the security of other systems, ITS has the authority to access, and inspect the configuration of, devices and equipment on that network and to require the immediate removal of any devices or equipment that it believes could be the source of the problem. ITS also has the authority to disable any or all of the local network, as necessary, to diagnose and/or remove the source of the problem.

6. Design

The network must be designed and configured to deliver high performance and reliability to meet the College's needs whilst providing a high degree of access control and a range of privilege restrictions.

7. Security

7.1 The network shall be segregated into separate logical domains with routing and, where appropriate, access controls operating between the domains. Where this is not yet the case, there shall be plans in place to address this. Appropriately configured firewalls shall be used to protect the segments comprising the College network.

7.2 All parts of the College shall be protected by an institutional firewall.

7.3 At a minimum, a policy of "default deny inbound" and "default permit outbound" will apply at an institutional firewall. Servers which are required to be accessible from outside the College will need to be registered and approved by Birkbeck Information Security. ITS will require full details of the server and data to be stored on it, as well as the details of the system owner. Services visible publicly must be run from a DMZ. ITS reserve the right to run security tests on the server and require that any vulnerabilities are addressed **prior** to any access being granted.

7.4 New applications and systems must transmit and/or accept passwords or other authentication credentials only if strongly encrypted. Existing uses of clear-text authentication must be disabled as rapidly as practicable. If this is not possible, contact Birkbeck Information Security.

7.5 Birkbeck ITS have the authority to disconnect systems considered insecure or pose a security risk to other parts of the Birkbeck infrastructure.

8. Network Access

8.1 Access to the resources on the network must be strictly controlled to prevent unauthorised access. Access control procedures must provide adequate safeguards through robust identification and authentication techniques. See the associated Code of Practice. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.

8.2 Remote access to the network will be subject to robust authentication and VPN connections to the network are only permitted for authorised users ensuring that use is authenticated, and data is encrypted during transit across the network. See the associated Code of Practice.

8.3 Moves, adds, changes and other reconfigurations of users' network infrastructure will only be carried out by ITS according to the Code of Practice.

9. Wireless

9.1 All wireless access to the College network must be authenticated and logged. (Any exceptions need to be agreed with ITS and will be registered and noted on the risk register.) As for wired infrastructure, appropriate logs must be kept so that it is always possible to determine who/what was using a particular IP address at a particular time (accounts must never be shared). Logs shall be retained for as long as is necessary and a record kept of how long each set of logs is kept.

9.2 Requirements for new wireless connectivity should be arranged with ITS as per the Code of Practice.

9.3 Users must not provide wireless networks within the College campus. This means users must not plug in anything that will act as a wireless access point even if they do not connect to the College network, as they may still interfere with other wireless provision and/or provide unsecured access to the Internet and, thus, pose a risk to the College. Birkbeck Information Security retain the right to disable (without notice) any 802.11 wireless device they identify as being unauthorised.

10. Risk Management

Any requests to Birkbeck Information Security and/or Birkbeck ITS for exceptions to the above, once approved, need to be identified within the appropriate Risk Register. Sufficient details need to be maintained in the register to ensure that mitigations are clearly identified, and any improvements or remedial activities required can feed into future budgeting and project management activities. Some exceptions may be approved as a frequent and generic activity.

This should be complementary to any risk management activity arising from the obligations set out in section 9 of the main BBK Information Security Policy.

11. Version Control

This policy replaces an earlier policy entitled Network Security Policy (last reviewed 2016).