Information Services

Birkbeck Information Security Policy

Supporting Policy 7: Birkbeck Information Security Roles and Responsibilities Policy

Approved by Strategic Planning Committee

4 July 2022

0. Context

This document 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 Information Security Roles and Responsibilities Policy sets out the foundation upon which good information security is built. The different organisational units in the College must carry out security and risk management, ensuring the appropriate policy and standards are applied consistently to continually improve the security posture of the College. All schools and professional services departments retain responsibility for ensuring Information Security in their areas. The key principle here is, information security is everyone's responsibility and an integral part of everyone's role. This enables the College to operate flexibly, effectively and securely.

2. Scope

This Policy applies to all individuals who use or access Birkbeck's Information or IT Resources.

3. Purpose

The purpose of this policy is to establish the appropriate protective security roles and responsibilities in the College. This policy has been developed to ensure that an effective risk based approach to security is being taken across the whole organisation. Employees and contractors must fulfil their information security responsibilities.

4. Policy Statement

4.1 Responsibilities of all users

All users must adhere to Birkbeck IT Regulations. Employees and contractors must meet their contractual agreements with the College and fulfil their responsibilities for information security.

Authorised users have access to IT facilities (e.g. computers, printers, software, email, network services and cloud services etc.) located at Birkbeck and other sites. With these facilities there are direct and implied responsibilities on the part of the College and of the user. Some of the responsibilities are highlighted here but users are advised to read and understand the relevant policies in the Birkbeck IT Regulations.

4.1.1 User ID/Password

- Authorised users are allocated a username and password, and must ensure that nobody else uses it. The user is responsible for the confidentiality of the username and password.
- Users must not use anyone else's username/password.
- Users must not obtain or try to obtain anyone else's password.
- Users must inform IT immediately if they suspect someone else of using their user ID/password.
- Users must lock their account, or use a password protected screen-saver if they wish to leave a computer unattended for a short period of time.
- Users must log out of shared computers if they do not intend to return within a short period of time.

4.1.2 Filestore, including cloud data storage

- Users must not gain access or attempt to gain access to any files owned by someone else unless the owner (or school/dept system support staff) has specifically granted access (in line with Birkbeck's IT Account Monitoring and Access Policy).
- Users must not use equipment in contravention of the law.
- Users must use anti-virus products (and keep them up to date) and must not introduce malicious code including viruses, network worms, Trojan horse, logic bombs etc.
- User must not download or install software/hardware which could be used to scan, attack or compromise security or service.

- Users must not install software on shared equipment which may interfere with the normal operation of that equipment.

4.1.3 Email

- Email should be treated in the same way as ordinary mail and the same standards of behaviour apply.
- Email which is confidential or of a sensitive nature should not be sent via email unless appropriate precautions are taken (seek advice from Birkbeck Information Security).
- Users must not transmit email that causes 'annoyance, inconvenience, or needless anxiety to other people'.
- Users must not send or attempt to send forged email.
- Users should contact ITS if they receive mail which they find offensive. The original message should not be deleted.

4.1.4 Network

- Users must not deliberately interfere or attempt to interfere with the operation of the network or computer systems.
- Users must not connect equipment to the College wired data network without authorisation from School Systems Support staff or ITS.
- Users must not operate any equipment or software designed to eavesdrop on wired or wireless network communications.

4.2 Additional responsibilities

In addition to the above, different groups of users have some responsibilities specific to their roles for ensuring information security.

4.2.1 Responsibilities of systems administrators (in schools)

Nominated Systems Administrators are responsible for the secure operation of the IT facility. This may be an individual responsible for a collection of systems, or the user who normally uses the system (in particular for office equipment). The responsibilities of system administrators include:

- Installing and maintaining the operating system and network connection in order to reduce the chance of unauthorised access.
- Ensuring that systems security patches are kept up to date where possible and such that the service is not adversely affected.
- Monitoring systems in order to detect breaches in security. In the event of any breach IT Services must be alerted.
- Restricting the use of privileged accounts. Users including systems administrators, should normally log in with user IDs without unnecessary (“superuser”) privileges. Privileged accounts should be used only for systems administrative work and monitoring.

- When undertaking systems work demanding privileged user status, administrators should log in under their own account before assuming privileged status (to maintain audit information).
- Ensuring that all software is properly licensed.
- Ensuring adequate backup procedures are in place.
- Ensuring adequate virus protection software must be installed.
- Changing passwords regularly and restricting knowledge of the super-user password.
- Providing a copy of superuser and system administrator passwords to ITS or School/ Dept Computer staff for use in emergency.
- Maintaining logging information, and in particular a record of log-ins on the computer, for one year.
- Administrators must not amend any audit or system information which may be used as part of an audit trail in cases of security breach.
- If necessary to protect or maintain service, administrators will disconnect a system, individual workstation, or software from the School.
- Monitoring activity and/or record traffic on the network if appropriate, including periodic intrusion detection testing either internally or by third party.
- Ensuring that adequate security is utilised when connecting out of band equipment to allow remote management/troubleshooting.

Administrators should also operate within the guidelines of the Charter for System and Network Administrators prepared by Jisc https://community.jisc.ac.uk/library/janet-services-documentation/suggested-charter-system-administrators).

4.2.2 Responsibilities of IT Services

In addition to the above (for systems maintained by ITS), ITS will also:

- Liaise with external organisations in the development and maintenance of the network.
- Inform system administrators of security information, hacking attempts, tools etc via an email list.
- Provide information and good practice guidelines.
- Assist School/Dept Systems Administrator to correct a security or breach, especially where the integrity of the network may be at risk, or it is affecting systems elsewhere.
- If necessary to protect and maintain service, disconnect a system, individual workstation, software, school network or building from the wider College network.
- Monitor activity on the network, including periodic intrusion detection testing either internally or by third party. If during a scan an obvious weakness is found, ITS will provide advice and assistance to the appropriate systems administrator.
- If no administrator is available, depending on the nature of the loophole, the offending system may be disconnected from the network.
- Maintain central checking of malicious code, including of email passing through central mail systems.
- Maintain site licences of virus protection software.

- Coordinate the development and maintenance of the security policy.
- Maintain perimeter firewall and internal rules to protect the College's IT infrastructure.

5. Version Control

Version	Date	Author	Comments
0.1	27 October 2020	Abu Hossain	First draft. Content rearranged from policy previously known as Network Security Policy.
0.2	29 April 2021	Reviewed by Abu Hossain	Added the context section.
0.3	16 February	Reviewed by Marion Rosenberg	Minor edits for completeness, accuracy and consistency.