UNIVERSITY OF CAMBRIDGE

School of Clinical Medicine Information Security Policy

High level policy

UNIVERSITY OF CAMBRIDGE

1. Document Control

Rev.	Author	Date	Comments
0.1	Richard Bartlett	23 Mar 2016	Submitted to School IT Committee for approval
0.9	Richard Bartlett	19 Apr 2016	IT Committee approved document submitted to Council of School

2. Purpose

This 'top level' information security policy sets out areas of risk which all School IT Service Providers should review and address, to ensure that appropriate information security policies and procedures are in place across the School.

This policy does not stipulate the content of any policy or procedure, but rather the outcomes which they should deliver. This should provide the School with sufficient assurance that appropriate and effective information security measures are in place, whilst allowing for each institution to take those measures they deem appropriate under their own responsibility.

3. Scope

This policy covers all Institutions under the School of Clinical Medicine. Regardless of where data is stored by the Institution, it is the responsibility of that Institution to ensure that appropriate policies and procedures are in place to protect the data gathered, stored and processed as part of their activity.

Where data is held on central University business systems (e.g. CUFS, CamSIS, CHRIS, X5 etc.) then the policy of that system applies, but wherever data is stored on institution central or local systems then their policies should apply.

4. Responsibilities

Institutions have a responsibility to put in place appropriate and proportionate measures to comply with the UK and EU data protection legislation, contracts the University has with data providers (e.g. the HSCIC) or the Trust, and research grant provisions. Against that they have to balance their responsibility to facilitate research, teaching, and administration, and uphold the University and School's core values of freedom of thought and expression.

Users have a responsibility to comply with any policies, procedures or working practices which their Institution puts in place to protect the systems and data under its care.

5. Requirements

All School IT providers should have policies and procedures to address the following areas of information security risk. Each requirement could be covered by a specific policy, or as one element of a larger policy.

5.1. Acceptable Use

To protect users and data from harm caused by misuse of Institution IT Systems, a definition of acceptable and unacceptable behaviour on the network should be defined in policy. Any local policy

should comply with the Rules Made by the Information Services Committee[1], and the terms of the provision of the JANET service[2]. There should be some process through which all users are made aware of this policy, if possible with their explicit acceptance of the policy being recorded.

5.2. Access control

To ensure that proper care has been taken to protect data and systems, policy elements should define how access to systems and data is granted, monitored and revoked. As far as possible the principle of least privilege should be followed, bearing in mind the relative freedoms required by Academic Research staff in the course of their work. Due regard should be paid to the Data Protection Act Seventh Principle[3] and any other legislation which may be applicable to the research activity of the institution. It may be appropriate to include information about how unauthorised access is prevented, detected and responded to.

5.3. Authentication

To comply with the most fundamental principles of information security[4], and the Rules made by the Information Services Committee[5], users with access to systems and data should be authenticated. Policy elements should address how users authenticate themselves, and what controls are put in place to manage the risks associated with authentication methods. In particular, any local policy should define a password policy which addresses the risk of credentials being used by someone other than the intended party (either through being compromised, shared between users, or re-used on non-University systems which are then compromised). Where appropriate, two factor authentication may also be stipulated in policy to protect data or systems which are particularly sensitive.

5.4. Data Handling

General best practice in handling administrative and research data should be embedded within the conditions of grant funded research, administrative processes or other local guidance. However, the measures which should be taken to protect data being received, captured, created, stored and processed by an institution should be defined. In particular, appropriate locations should be defined for different categories of data according to their sensitivity and value. The more sensitive or valuable data is the more care should be taken in the way it is handled. Specific attention should be paid to use of portable storage (encrypted and unencrypted), single copy storage on local disk, and central storage.

5.5. Email

Email is a significant source of risk of information security breach, through malware and phishing, and also information leakage through human error, or lack of awareness of appropriate communication methods for different types of data. Policy elements should address how attachments to emails are handled (both by any systems level protection but also by guidelines for staff), and any restrictions on

[1] http://www.uis.cam.ac.uk/governance/information-services-committee/rules-and-guidelines/rules
[2] https://community.jisc.ac.uk/library/janet-policies/terms-provision-janet-service
[3] https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
[4] http://systems.hscic.gov.uk/infogov/security
[5] http://www.uis.cam.ac.uk/governance/information-services-committee/rules-and-guidelines/rules

email including what content can or cannot be sent, or which recipient addresses can or cannot receive certain content.

5.6. Incident Response

A process should be defined which is followed in the event of a security incident. That process should define what triggers incident response, the roles and responsibilities of those involved in incident response, the process for recording, investigating, analysing, mitigating, resolving and preventing incidents, and the reporting which may be required both internally and externally (e.g. compliance with School Incident Management and Reporting Procedures[6] or University Information Services CERT procedures[7]).

5.7. Mobile Computing

With the proliferation of mobile devices (smartphones, tablets and laptops), many of which are not directly managed by Institutions, it is important that the risk these devices may present is assessed, and appropriate controls put in place to prevent data loss, release, or unauthorised access. In particular, Institutions should ensure that any devices connected to their network or the University network are appropriately authorised and authenticated, and that staff are aware of what is and is not appropriate to store (directly or indirectly as contents of email) on their mobile devices. Encryption may be used as a risk reduction measure to allow users flexibility of access whilst protection the Institution's (and their own) data and privacy.

5.8. Monitoring and Logging

All institutions should monitor and log activity on their network to the extent needed to provide assurance that only authorised persons are accessing the data the Institution is responsible for. However, it is very important that the level of monitoring and logging is proportionate, and all users of Institution systems are informed about what is logged, for what purposes, and how long that data is retained. An Acceptable Use Policy (see 4.1 above) could contain user facing information about the nature of logging, but a specific policy on what is logged, why, how that data is stored and protected and when it is destroyed is an important protection for the Institution and its staff.

5.9. Remote Access

University staff and students, and researchers in particular, depend upon remote access to Institution systems. That capability expands the systems which connect to the network significantly, and increases the risk of unauthorised network access accordingly. A Remote Access Policy should address that risk, defining the permitted remote access methods, the process through which people are granted remote access, and any measures which are taken to prevent unauthorised access.

6. Management

All Institutions under the School should confirm that they have put in place measures to comply with this School Information Security Policy, and should submit those documents to the School Information Security Oversight Committee (SISOC) as evidence to support that assurance. Where policies and

[6] http://www.medschl.cam.ac.uk/research/information-governance/incident-management-and-reporting-procedures/
[7] http://www.ucs.cam.ac.uk/security/reporting/inside.html

procedures do not already exist sample templates can be provided, and the SISOC may call upon expertise within the School or the University to assist Institutions in developing the necessary policy framework. It is desirable that policy within the different School Institutions converges over time to reduce the burden of administration, facilitate collaboration between Institutions, and improve the efficacy of governance in this area overall.