Information Security Oversight Committee Meeting

Tuesday, 5th July, 2016

Present: Richard Bartlett (RB)
Lydia Drumright (LD)
Kieran Lovell (KD)
Stephen Jones (SJ)
Guy Williams (GW)
Jonathan Wilson (JW)
Richard Hutchinson (RH)
Peter Maccallum (PM)
Carolyn Read (CR)

1. Apologies: Stefan Graf (SG)

2. Terms of Reference

RB highlighted and clarified a number of matters:

- The University’s Acceptable Use (AU) policy is evolving at present and not yet finalised (item 3.2) and this may inform provider level policies.
- CR will responsible for approving and reviewing the implementation of any safe havens under the School’s Information Governance Toolkit (ITG) (item 3.2)
- The proposed review of information security breaches would cover breaches in any safe haven (item 3.2)
- Meetings will be held on a termly basis i.e. one per term and more if necessary (item 6)

The Committee also agreed that they should keep up to date with current threats and a review of these threats should be added to the standing agenda items for each meeting.

The Committee then discussed whether groups outside the School (especially in SBS) could have access to the School’s safe havens. CR said she did not want groups outside the School using the School’s IGT.

Action Point - RB to take this matter up with the Information Governance Working Group of the NHS-HE Forum as they are responsible for reviewing the School’s toolkit.

RB added that if groups outside the School want access to a safe haven then their first port of call should be the UIS.

Action Point – LD to speak to Rhys Morgan at the Research Office about this issue.

3. Objectives

i) Setting Policy

A discussion took place on the AU policy. LD noted that it was not easy to find information on this policy and RB told her that he intended to put all this information in an IT directory on the School’s website. He added that that this directory should contain AU policies from all School IT providers.

Action Point – KL to create Drupal page and everyone to put their AU policies on this page. Everyone to review the different policies and discuss at the next Committee meeting.
Action Point – KL to come up with justification for no use of cloud storage for PID (OneDrive and DropBox)

Action Point – RB and KL to make sure any UIS or CSCS website guidance comes up on Google search rankings.

Also with regard to the AU policy, RB also raised the issue of security for mobile devices. He said that CSCS was become increasingly concerned about this issue and he was keen to find out whether these devices presented a real security risk in which case they would need to amend the AU policy.

Action Point – KL to contact the Computer Lab about this issue and report back to the rest of the Committee.

The Committee also discussed staff inductions and agreed that the AU policy should be included in all staff inductions.

Action Point – CR to speak with Jackie Hall about staff inductions to ensure that new staff are made fully aware of the AU policy.

ii) Review and Implementation of Safe Havens.
RB said that the Committee needed a common overview as to how this might work and he suggested that a “light touch” ISO audit involving peer review might be the way forward.

Action Point – RB to draft high level document to set out how this would work and upload it to the Drupal page.

A discussion also took place on who could check the security for each safe haven. It was agreed that peer review was an appropriate mechanism, according to the procedures which RB would draft (see 3ii above). UIS may also be able to provide expertise in this area.

Action Point – KL to look into this matter and find a security specialist at the UIS who would be able to carry out security testing (including password testing).

The Committee agreed that they would agree an approach on or by the next meeting and the reviews should be carried out within the next 9 months (i.e. before the next cycle of the IGT).

iii) Maintaining the Information Governance Toolkit
RB confirmed that all safe havens would need to confirm compliance with the current version of the Information Governance Toolkit by March 2017, and the next version of the toolkit, with substantial changes, was expected in 2017.

iv) Reviewing Breaches
RB informed the Committee that the current policy regarding breaches is on the School's website. A discussion then ensued on the definition of a breach. It was agreed that breach reporting should be local in the first instance to reduce reportee anxiety, then channelled to the appropriate University authorities.

Action Point – RB to come up with a definition of a breach and amend the current policy accordingly.

The Committee also discussed how breaches should be handled from an HR perspective. They agreed that there should be a “soft” approach for staff who self-reported any breaches, and in most cases no further action would be taken. However the position would be far more serious for staff who did not report or recognise their breaches.

Action Point – RB to discuss with Gail Christey how breaches should be handled from an HR perspective.

4. AOB
   None

5. Date of next meeting
   TBC for mid to late October.