2nd December, 2016, Committee Room, Bay 13, (s202)

Present: Richard Bartlett (RB), Carolyn Read (CR), Peter McCallum (PM), Stephen Jones (SJ), Rich Hutchinson (RH), Stefan Graf (SG), Guy Williams (GW), Kieran Lovell (KL)

INFORMATION SECURITY OVERSIGHT COMMITTEE (ISOC)

1. Apologies
Lydia Drumright (LD), Jonathan Wilson (JW)

2. Minutes
The minutes of the first meeting (5th July, 2016) were approved.

3. Actions from the last meeting

(a) **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.** The lack of single authoritative contact within SCM for the toolkit is included as an issue within the report sent on behalf of the NHS-HE Working Group by Bridget Kenyon, see section 2.4 for example.

(b) **LD to speak to Rhys Morgan at the Research Office about access to a safe haven for those outside the SCM.** No update from LD, but CR said that LD was pushing for a policy at University level.

(c) **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.** Completed, but on Moodle, and no data has been uploaded yet. RB highlighted the CSCS AUP at https://cscs.medschl.cam.ac.uk/about-us/policies/cscs-aup/, and suggested he collect the remaining Institution AUPs and put them in an alternative space. KL raised the Regulation of Investigatory Powers Act (RIPA) as IT providers may be in scope (which would impact policy), he will raise this with Martin Bellamy for discussion with UCISA/JISC/Legal Services.

(d) **KL to contact the Computer Lab about mobile device management (MDM) and report back to the rest of the Committee.** KL reported back that the Computer Lab were against any sort of control, and no solution was yet identified. RB has raised this requirement at the Information Security Management Programme (ISMP) and will continue to follow up.

(e) **CR to speak with Jackie Hall about staff inductions to ensure that new staff are made fully aware of the AU policy.** This was discussed at School SMT, SG said the Haematology
induction is excellent, RB/CR to bring this to Caroline Newman (acting School HR Business Manager) as the quality bar to be met.

(f) **RB to draft high level document to set out how peer review ‘light touch’ audit would work and upload it to the Drupal page.** This had not yet been done, due to lack of resource (RB) in CSCS, and a lack of free resource elsewhere. KL is going on a course which covers audit in the syllabus, action on RB/KL to come up with a proposed approach.

(g) **KL to look into external penetration testing and find a security specialist at the UIS who would be able to carry out security testing (including password testing).** Not yet completed, but some progress had been made with the Ethical Hacking group.

(h) **RB to come up with a definition of a breach and amend the current policy accordingly.** Definition of breach from the Information Security Management Programme (ISMP) discussions unclear, RB is currently using [https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance_V5%201%20290515_Final_Publish.pdf](https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance_V5%201%20290515_Final_Publish.pdf), which is a reasonable interpretation of that could be "unlawful access, disclosure or misuse of confidential data, or information security breaches which did or could have led to such an incident".

(i) **RB to discuss with Gail Christey how breaches should be handled from an HR perspective (breach reporting should be local to reduce anxiety, then channeled to the authorities, and handle self-reporting and non-reporting appropriately).** This was discussed at ISMP, I stressed current reporting framework as approved at ISM-SC needed to maintain parallel reporting lines (local IT and CERT), to ensure no barrier to reporting. RB raised with HR and should meet soon.

4. Objectives

(a) Setting Policy
RB introduced the UIS Organisational Framework for Information Security, and the UIS Information Loss Reporting Framework (see accompanying paper slide 2). CR asked when James Knapton (University Data Protection Officer) gets involved, RB confirmed James had been consulted on its development by UIS Information Management.

(b) Policy Development Process
RB outlined how this is intended to work for web hosting policy (see attached paper slide 4, Draft 0.x > Small Review Group > Large Review Group > ISM-SC > ISC for final approval).

(c) CSCP incident, NetNames and Web Hosting Policy
The Cambridge School Classics Project, resulting procurement of the NetNames Service and the aborted Web Hosting Policy were all covered above.

(d) Review of Safe Havens
There is not a lot of resource to review existing Secure Data Hosting implementations by the end of February. KL suggested one fast/easy option would be certification to Cyber Essentials Plus, (cost <£1k). RB will raise the fact that we don't have enough money and/or resource to do this at School level. We've changed the way some of the toolkit implementations works, more work to be done. User consultation with Research staff key to designing and developing these systems. It was noted that GP's are often not informed about good/best practice in exchanging data (in one case at least a CCG had to be informed when
PID went from the nhs.net email service to the cam.ac.uk email service, which is in effect an information security breach).

(e) Maintaining Information Governance Toolkit
There has been quite a lot of detailed policy change to allow for new use cases, will make the implementation review difficult, but required to ensure the system meets the needs of users.

(f) Review Breaches
No breaches were known (within the Secure Data Hosting environments), the question was asked, “How do we find out if there’s a breach?” SG said he has collaborators who store data on the HPC, they sign a document that says they won't copy data out, but from his conversations with Stuart Rankin, verifying this is really hard to do, as there are too many egress points. RB said that where it needs to be possible to extract some approved data from a secure environment there were technological options for ensuring that was possible, if you control the egress points.

(g) Review threat landscape
Ransomware is still the highest known risk, whilst healthcare is not being explicitly targeted it is suffering from such infections due to environment specific attack vectors (e.g. DHL/FedEx shipment emails are more credible on the Biomedical Campus).

5. Any other business

- RB asked if there were any potentially effective solutions to security challenges which people were aware of, none were reported.
- Training and awareness of staff.
  RH said they were happy with their user’s awareness, though staff in the field were more of a challenge. GW pointed out it depends on the user, some (e.g. Radiographers) are more aware, some less so. SG said technical users were well aware, in some cases they had signed agreements, a lot of their data is read only, with only restricted groups having access. Stuart Meacham does awareness raising every 2-3 weeks.
- Consultation methods
  Research Nurses need to be happy that systems work for them. One example of a bad implementation was the revocation of SDHS accounts not warning users before execution, if CSCS issued warnings first they would be happy with that. RB noted this request.

6. Date of next meeting
The next meeting will be arranged by Pippa (CSCS Department Administrator) by circulation.

7. Actions
(a) LD to speak to Rhys Morgan at the Research Office about access to a safe haven for those outside the SCM
(b) RB collect the remaining Institution AUPs and put them in an alternative space
(c) KL raise RIPA with Martin Bellamy for discussion with UCISA/JISC/Legal Services
(d) RB follow up requirement for Mobile Device Management with ISMP
(e) RB talk to Caroline Newman ref School Inductions and using Haematology as quality bar
(f) RB to draft high level document to set out how peer review 'light touch' audit would work
(g) KL look into external penetration testing and find a security specialist at the UIS who would be able to carry out security testing (including password testing).
(h) RB talk to HR about procedure for breach reporting to ensure everyone was encouraged to report breaches without fear of penalty

(i) RB raise lack of funding and/or resource to do safe haven review/audit at School level