St George’s, University of London

Compliance Audit Procedure

1 Introduction

1.1 The purpose of the audit is to assess compliance with SGUL information governance (IG), data protection and information security related policies.

1.2 The audit will check and confirm that standard operating procedures are being adhered to.

1.3 The scope of the audit will include both physical and logical information security and access controls.

2 Responsibility

2.1 Compliance spot audits will be conducted by the University’s IG leads, or a delegate on their behalf, on a monthly basis during normal working hours. SGUL security patrols will carry spot checks during their security patrols during non-normal working hours.

2.2 All Directors in their capacity as Information Asset Owners (IAOs) are ultimately responsible for ensuring audits of compliance are routinely carried out in their divisions.

3 Audit Process

3.1 The IG lead will identify a different team, office or group of offices within their division to carry out a ‘spot check’ audit each month.

3.2 The IG lead, or a delegate on their behalf, will feed back on their findings to staff in the audited areas and agree an appropriate timeframe for rectifying any compliance issues, where relevant.

3.3 The IG lead, or a delegate on their behalf will then follow up on the recommended rectification measures to ensure they have been implemented.

3.4 The monthly ‘spot checks’ should be completed using the template in Appendix A of this document. The IG lead should also use the form to keep a record of the areas that have been checked.

3.5 The IG lead will escalate significant compliance issues highlighted by the monthly audits to the Information Asset Owner and / or the SIRO.

3.6 If necessary the IG lead may also seek advice from the Information Governance Manager or Data Protection Officer on any compliance concerns.

3.7 IG Leads will submit the findings of their ‘spot checks’ to the Data Protection Officer to be reviewed to ensure any issues identified are addressed and action is taken.

3.8 Once a year a more comprehensive audit will be carried out. It is proposed that this might form part of the Annual Internal Audit Plan (to be confirmed). The Annual Audit Review will focus on the broader requirements of information governance, and it is likely that this will include an assessment of staff knowledge with regard to information governance, data protection and information security.

Appendix A IG Lead Compliance Spot Audit Template

Institute:	PI / Location (s):	Date:

Compliance Check	Yes	No	N/A
PC: do all users log out / of lock screen when PC is left unattended? *(IT Conditions of Use (5.1 Protect Identity)*			
If No, please remind staff that when left unattended PC should be locked using the Windows-L key combination.			
Comment:			
Photocopiers/ printers / fax: has any confidential information[1] been left in these devices? *(Clear Desk & Screen Procedure)*			
If Yes, please remind staff that all confidential information should be collected from printers/photocopiers as soon as possible			
Comment:			
Clear desk: has any confidential information been left in plain sight on desks when staff have left the office? *(Clear Desk & Screen Procedure)*			
If Yes, please remind staff that all confidential information should be locked away when desk is unattended			
Comment:			
Post rooms: has any confidential information been left here?			
If Yes, please remind staff that confidential information should be not be left in post rooms			
Comment:			
USB Sticks: are all USB sticks containing confidential information encrypted and stored securely? *(IT Conditions of Use {7.1.2 Removable media and mobile devices})*			
If USB sticks are used with confidential information then they must be encrypted and stored securely. Unencrypted USB sticks should not be used to store confidential information.			
Comment:			

[1] Confidential Information covers personal identifiable information and sensitive business / research critical information.

Compliance Check	Yes	No	N/A
Laptops: Are non-SGUL laptops used for confidential information? *(IT Conditions of Use {7.1.2 Removable media and mobile devices})*			
If Yes, ensure the laptop is encrypted. Unencrypted personal devices should not be used to store or process confidential information at all.			
Comment:			
Whiteboards: has confidential information been left on display here?			
If Yes, please remind staff that all confidential information should be removed from whiteboards after use			
Comment:			
Confidential waste: is confidential waste appropriately destroyed? *(Secure Disposal Procedure)*			
If No, please remind staff that (i) an approved confidential waste service should be being used, (ii) shredders, if used, should conform to an appropriate standard. (iii) confidential waste awaiting destruction is to be securely stored until collection.			
Comment:			
Access to personal information- paper files: can hard-copied confidential information be accessed when not being used? *(Clear Desk & Screen Procedure)*			
If Yes, please remind staff that any confidential information should be kept in locked drawers / cabinets when not being used			
Comment:			
Access to areas: are physical security mechanisms working correctly? e.g. keypad locks in place, broken locks have been reported / not left unfixed *(Key Policy)*			
If No, please remind staff that any fault should be reported to Estates. List broken door locks in comments.			
Comment:			
Key management: is a storage box used to store keys securely?			
If Yes, please ensure the storage box is secure and there is a suitable procedure to control key distribution.			
Comment:			