SLMS Incident Reporting Procedure

1 Document Information	
Document Name	SLMS-IG15 SLMS Incident Reporting Procedure
Author	Trevor Peacock
Issue Date	04/06/2018
Approved By	Chair of SLMS IGSG
Next review	Three years

2 Document History		
Version	**Date**	**Summary of change**
0.1	21/02/2013	First draft for discussion
0.2	19/03/2013	Second draft with derivations from Information Security procedures
0.3	06/06/2013	Revised with input from Bridget Kenyon
0.4	02/07/2013	Revisions from IG Toolkit v11 at Section 4 and Appendix 2.
1.0	02/08/2013	Approved by Chair of SLMS IGSG
0.5	05/06/14	Amendments to reflect separate processes for Safe Haven and all other information incidents. Also included escalation process approved at IGSG 06/05/2014
2.0	12/06/2014	Approved by Chair of SLMS IGSG
2.1	19/02/2015	Amendments to clarify reporting of incidents and corrective actions. Out of date contact details removed.
3.0	20/03/2015	Approved by Chair of SLMS IGSG
3.1	08/06/2015	T Peacock: added requirement to report security weaknesses and also to feed back to users following security incident
4.0	12/06/2015	Approved by Chair of SLMS IGSG
4.1	08/02/2016	Reviewed to clarify actions, include comments from internal audit and remove incident management elements, covered elsewhere
5.0	22/02/2016	Approved by Chair of SLMS IGSG
5.1	31/05/2018	Reviewed by IG Lead and IG Officer
6.0	04/06/2018	Approved by Chair of IG Steering Group

Information Security Incident Reporting

3 Introduction

Information security is everyone's responsibility; the SLMS needs to manage information security incidents to meet legal, contractual and regulatory obligations. A mishandled information incident will have a broad impact upon the SLMS's ability to undertake research.

4 Objective

The objectives of this procedure are for the SLMS to: meet its legal obligations; respond appropriately and minimise the impact of information security incidents; ensure that lessons are learnt and acted upon to continually improve controls that reduce the risk of reoccurrence.

5 Scope

This procedure applies to confidential research data being processed by or on behalf of the SLMS

This procedure applies to UCL employees, students, honorary contract holders, contractors and third parties handling data within and on behalf of SLMS.

6 Responsibilities

Persons defined in the scope above shall identify information security incidents, near misses and weaknesses involving services or systems within the SLMS and report them as detailed below

The IG Lead will be responsible for onward reporting and coordinating other teams as appropriate

Where there is a suspicion of criminal activity, it is critical that evidence is preserved. Please see appendix A before proceeding

7 Definitions

7.1 Information Security Incident

An information security incident is any violation of the UCL Information Security Policy, SLMS Information Governance (IG) or UCL Data Protection Policy. An information security incident can be defined as any event that has an adverse impact and results in accidental or deliberate:

- Unauthorised disclosure of confidential information
- Damage to the integrity of a system or data
- Loss of availability of a system or data

Examples of adverse impacts include:

- Threat to personal safety or privacy
- Legal, regulatory or contractual obligation or penalty
- Financial loss
- Disruption to SLMS business
- Reputational damage to SLMS

Examples of security incidents:

- Using another user's credentials to gain unauthorized access
- Unplanned outage of information systems
- Confidential printed material left in open view
- Theft or loss of IT equipment
- Malware infection
- Inadequate disposal of confidential material

7.2 **Near-miss**

An unplanned event that did not result in an impact, but had the potential to do so; only a fortunate break in the chain of events prevented the adverse impact

7.3 **Vulnerability**

A weakness with the potential to be exploited and cause an incident

8 Reporting of Security Incidents

The following applies to all security incidents. Where there is a suspicion of criminal activity, please see appendix A before proceeding.

8.1 **When**
Information security incidents must be reported as soon as possible after they occur, or have been identified. UCL is legally obliged to report data breaches to the Information Commissioner's Office (ICO) within 72 hours from initial detection. It is imperative that reports are sent immediately after an incident so that this can be achieved; if there is a delay between an incident occurring and the discovery of said incident, it must still be reported.

8.2 **What**
For all incidents, the report must give as much detail as possible.
Only include personal details in the report where this is necessary and justified.

8.3 **How**
Incidents must be reported via the routes detailed in this procedure, even if other reporting routes are in use

8.4 **To Whom**
Incidents must be reported via the Information Security Group:
https://www.ucl.ac.uk/informationsecurity/itsecurity/incidentresponse

9 Corrective actions and continual improvement

The IG Lead will coordinate work to fully assess the impact of an incident, establish the root cause to enable follow-up work that addresses and reduces the risk of reoccurrence

As an output from the incident reporting process and where it is appropriate to do so, feedback on the cause of the incident, actions taken to address it and any required local actions will be provided to the end user and the Information Asset Owner

Broader improvements or changes affecting more than one study will be reviewed with the Data Safe Haven User Group, amongst other stakeholders

Appendix A

Criminal misuse

Where criminal activity is suspected, it is important to ensure that the scene of the incident is preserved. Do not switch off equipment or interfere in any way. If possible, take photographs of the incident scene paying particular attention to peripheral equipment and connections. Where practical, prevent staff or any third parties from accessing the incident scene.

Potential child abuse data

Do NOT view images or footage. Follow the guidance in the section on criminal misuse, above, and **contact** the Information Security Group immediately.