SLMS Incident Reporting Procedure

1 Document Information
Document Name: SLMS-IG15 SLMS Incident Reporting Procedure
Author: Trevor Peacock
Issue Date: 22/02/2016
Approved By: Chair of SLMS IGSG
Next review: Three years

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 Out of date contact details removed.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

3 Introduction

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

4 Objective

4.1 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

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

5.2 This procedure applies to UCL / SLMS employees, honorary contract holders, contractors and third parties.

6 Responsibilities

6.1 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

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

6.3 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

7.2 An information security incident is any violation of the SLMS Information Governance (IG) or UCL Information Security Policy. An information security incident can be defined as any event that has an adverse impact and resulted or could result in:

- The unauthorized disclosure of confidential information
- The integrity of a system or data being put at risk
- The availability of the system or information being put at risk

7.3 Examples of adverse impacts include:

- Threat to personal safety or privacy
- Legal obligation or penalty
- Financial loss
- Disruption of SLMS business

SLMS-IG15 Incident Reporting Procedure v5.0
Page 2 of 5
• Reputational damage to SLMS

7.4 Examples of security incidents:
- Using another user’s credentials to gain unauthorized access
- Unplanned outage of the SLMS Data Safe Haven
- Transfer of sensitive data to a personally owned device
- Unauthorised disclosure of information (either intentional or accidental)
- Theft or loss of IT equipment
- Malware infection
- Inadequate disposal of confidential material

7.5 Near-miss

7.6 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

7.7 Vulnerability

7.8 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, it is critical that evidence is preserved. Please see appendix A before proceeding.

8.1 When
8.2 Information security incidents must be reported as soon as possible after they occur, or have been identified. Reports sent immediately after the incident are likely to be the most valuable; if there is a delay between an incident occurring and the discovery of said incident, it must still be reported.

8.3 What
8.4 For all incidents, the report must give as much detail as possible.
8.5 Personal details should, wherever possible, be omitted.
8.6 Any policies or procedures which may have been breached shall be referenced in the report.

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

8.9 To Whom
8.10 Incidents relating to the operation of the SLMS Data Safe Haven shall be reported to the IG Lead slms.pid@ucl.ac.uk

9 Corrective actions and continual improvement

9.1 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
9.2 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.

9.3 Broader improvements or changes affecting more than one study will be reviewed with the Data Safe Haven User Group.
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.