Policy

Security Incident Reporting Information

Issued November 2011

The purpose of this document is to describe the procedures for identifying, reporting, responding to, and learning from loss of information and information systems e.g. laptops, USBs and hard copy files / documents.

The objective of Security Incident Reporting and Management is to detect, investigate and resolve any actual, suspected or potential breaches of information security, and to take action that will avoid, or reduce the impact or probability of a further similar reoccurrence.
# Document Information

<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Security Incident Reporting (Information)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reference number</strong></td>
<td>1/2/9/1</td>
</tr>
<tr>
<td><strong>Supersedes</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Date of issue</strong></td>
<td>November 2011</td>
</tr>
<tr>
<td><strong>Implementation</strong></td>
<td>November 2011</td>
</tr>
<tr>
<td><strong>Review date</strong></td>
<td>July 2014</td>
</tr>
<tr>
<td><strong>Review by</strong></td>
<td>AEO(PD), ICT &amp; Facilities Manager, SIRO</td>
</tr>
<tr>
<td><strong>Prepared by</strong></td>
<td>AEO(PD, ICT &amp; Facilities Manager, Corporate Governance Officer, ICT Systems Manager / ITSO &amp; LDPO …)</td>
</tr>
<tr>
<td><strong>Consultation</strong></td>
<td>AEO(PD, ICT &amp; Facilities Manager, Corporate Governance Officer, ICT Systems Manager / ITSO &amp; LDPO …)</td>
</tr>
<tr>
<td><strong>Supply / distribution</strong></td>
<td>Available as a read-only document on the intranet plus one hard copy to each school &amp; setting</td>
</tr>
<tr>
<td><strong>Other relevant approved documents</strong></td>
<td>JSP 440 The Defence Manual of Security SCE Information Management Strategy SCE AUP</td>
</tr>
<tr>
<td><strong>Approved by</strong></td>
<td>Agency Executive Board (November 2011)</td>
</tr>
<tr>
<td><strong>Authorised by</strong></td>
<td>SIRO / DCE</td>
</tr>
</tbody>
</table>
1. **Purpose**

1.1 The purpose of this document is to describe the procedures for identifying, reporting, responding to, and learning from loss of information and information systems e.g. laptops, USBs and hard copy files / documents.

2. **Scope**

2.1 This procedure is applicable to all aspects of the Agency’s operations whether electronic, non-electronic, personnel, premises or infrastructure.

3. **Overview**

3.1 All systems and activities will be subject to formal incident recording and escalation procedures.

3.2 Incident recording will be used to log all unusual events. The mechanism will include what happened, what was done and final solution.

3.3 The objective of Security Incident Reporting and Management is to detect, investigate and resolve any actual, suspected or potential breaches of information security, and to take action that will avoid, or reduce the impact or probability of a further similar reoccurrence.

3.4 A security incident is an event which causes or has potential to cause:

- loss of system or information availability
- disclosure of confidential information, whether electronic or paper, or any other form including conversation
- corruption of information
- disruption of activity
- financial loss
- legal action.

3.5 Examples of incidents could include activity such as:

- the unauthorised use of a system for the processing or storage of data
- loss of removable media (USB Stick, Disc etc) and portable equipment (Laptops/Table, PCs)
- loss of paper files containing sensitive data.

3.6 The following should be established as rapidly as possible:

- when the incident occurred;
- when the incident was discovered
- details of the person reporting the incident;
- whether a near miss or an actual incident;
• what data and data media is involved;
• who is involved (e.g. individuals, schools);
• where the incident occurred;
• the sensitivity of the data and if personal data, the number of persons involved;
• whether the information and/or media was protectively marked and if so at what level;
• who is aware of the incident;
• whether and how the data might be used by a third party;
• the Information Asset Owner for the information involved;
• the immediate cause of the information loss e.g. breach, theft, misplaced, destroyed;
• the location of the information at the point of loss e.g. in the post, with a courier, in a SCE School/office;
  ◆ If in the post
  ◆ how was it sent?
  ◆ Was it double enveloped?
  ◆ Was the address verified?
  ◆ Where was it sent from?
  ◆ Was it double enveloped?
• If with a courier
  ◆ From where was it collected?
  ◆ Was it sent with “track and trace”?
  ◆ Was it collected by the expected courier?
  ◆ Was the address verified?
  ◆ Was it double enveloped?
• If from SCE School/Office
  ◆ From where was it accessed/stole? (e.g. terminal, public areas, desk, drawer, filing cabinet, office)
  ◆ Was it protectively marked?
  ◆ If it was protectively marked, was it stored appropriately?
• The crime number if the incident has been reported to the RMP/Police.

3.7 While each employee is personally responsible for ensuring that no security breaches occur as a result of their actions, everyone must be aware of their responsibility to report any potential, suspected or actual incident such as (security threats?), data loss, vulnerabilities, breaches, software or system failures to the IAO.

3.8 Security breaches caused knowingly by reckless behaviour, or non-compliance with Security Policies including the non-reporting of an incident, may result in disciplinary action.
4. Responsibilities

4.1 Users

- report any incidents promptly to the Information Asset Owner (IAO)
- provide further information or evidence when requested.

4.2 Information Asset Owner

- report all incidents to Lead Data Protection Officer (LDPO)
- report incident to School Governance Committee Chair, if appropriate
- complete Security Incident Report Form

4.3 Lead Data Protection Officer

- disseminate blank Security Incident Report Forms on request
- log and allocate reference for completed Security Incident Report forms
- report all incidents to Senior Information Risk Officer (SIRO)
- throughout the resolution period – keep the Incident Report Progress Record (spreadsheet) up to date
- maintain library of completed records

4.4 Senior Information Risk Officer

- allocate severity and priority to incident and agree resolution action plan
- monitor the resolution
- advise and involve other parties as appropriate (Chief Information Officer (CIO))
- review resolved incident and manage activities to avoid or reduce the probability of reoccurrence and the potential impact of future incidents
- approve closure of resolved incidents
- provide annual Process Owner’s Report to MOD CIO

4.5 ICT Systems Manager

- report data loss and hardware incidents to Joint Security Coordination Centre (JSyCC)

5. Procedure

5.1 This section describes procedure, but as every incident is different, common sense should be used to ensure that incidents are resolved with appropriate priority according to their severity.

5.2 Prompt action may be necessary to reduce the potential impact of an incident, so there may be times when an incident is resolved before it is recorded. If this occurs, an incident report form should be completed as soon as possible after the event.
5.3 It is important that every incident, however minor is recorded and follows this procedure to ensure that the probability of reoccurrence is avoided or reduced, and the impact of future incidents is minimised.

5.4 Recording

- Every reported incident will be recorded on a Security Incident report form (see Appendix A)
- LDPO will allocate a Reference Number and record the details on the Incident Report Progress Record
- LDPO will keep the records up to date as resolution progresses

5.5 Resolution

Once the incident has been recorded, it will be prioritised according to severity, which will be based upon the actual or potential impact of the incident upon the Agency’s systems and information and will be categorised as:

- Critical (C)
- High (H)
- Medium (M)
- Low (L)

Resolution of the incident will be allocated to an individual or team, and an action plan will be produced with target resolution times. The resources used to resolve the incident will depend upon the identified severity level. For example, in the case of a Low severity “no action” may be an acceptable option if the resources required outweigh the impact.

5.6 Escalation

Every security incident that may have an impact on schools, pupils, staff or parents will be reported immediately to the SIRO and the School Governance Committee Chair. If it is appropriate to do so the MOD CIO will be made aware of the incident.

On resolution of the incident, actions taken will be recorded on the Security Incident Report Form.

5.7 Review and Learning

All resolved incidents will be reviewed to ascertain whether there is a risk of reoccurrence. If there is no such risk the incident record will be closed. All potential vulnerabilities will be assessed, and appropriate action taken to ensure that the risk is kept to an acceptable level, implementing such controls as may be necessary.

- where appropriate risk registers will be updated.

5.8 Closure

Each incident will remain open until it has been satisfactorily resolved, documentation completed, and actions taken to avoid reoccurrence, or to ensure the impact of reoccurrence is at an acceptable level. Closure will be approved by the SIRO.
### Annex A - SCE Security Incident Reporting Form

Please use this form to report any breach of security e.g. break in, theft, loss of laptop or data

<table>
<thead>
<tr>
<th>Date of Incident:</th>
<th>Place of Incident:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Name of person reporting incident:</th>
<th>(in block capitals)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Brief Description of Incident:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Brief Description of Any Action Taken (at time of discovery):</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Date this Form Sent to HQ SCE:</th>
<th>Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(in block capitals)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature:</th>
</tr>
</thead>
</table>

Overleaf for LDPO Use
<table>
<thead>
<tr>
<th>Incident Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date this Form Received:</td>
</tr>
<tr>
<td>Date SIRO Informed:</td>
</tr>
<tr>
<td>Brief Description of Action Taken by LDPO:</td>
</tr>
<tr>
<td>Date of Follow-up &amp; Brief Description of Follow-up Action :</td>
</tr>
</tbody>
</table>
Annex B – Process Flowchart

1Information Asset Owner (Assistant Directors/Head Teachers/Head of CEAS)
2Senior Information Risk Officer
3Lead Data Protection Officer
4MOD Chief Information Officer
5MOD Joint Security Coordination Centre