STRONG HERITAGE | STRONG FUTURE
RHONDDA CYNON TAF
TREFTADAETH GADARN | DYFODOL SICR

INFORMATION MANAGEMENT

Procedure for investigating information security incidents / events

Version 1.0 (FINAL) wef 10.08.2016

Content

Appendix

Procedure for investigating information security incidents / events

In keeping with the Council's Information Security Policy (which can be found on Inform) a consistent approach to dealing with information security incidents and events must be maintained across the Council. Incidents and events must be appropriately handled and investigated in order to establish facts and any corrective and/or preventative actions required.

This guide outlines the procedure which must be followed when **investigating** an information security incident / event. It should be read in conjunction with the 'Procedure for **reporting** Information Security incidents / events' (which can be found on Inform under the Support Services > Information Management > 'Good Practice Guides' section).

1. Initial review of information security incident / event call by Information Management Team.

Once a call has been raised with the ICT Service Desk and classified as an Information Security call, it will be routed to the Information Management Team.

The Information Management Team will undertake an initial review of the call to determine whether it should be dealt with as an 'event' or escalated to an 'incident'.

The term information security incident / event is very broad and covers a wide range of situations which can vary considerably. Events are typically 'potential' or 'internal' breaches of security (policy / procedures etc), whereas 'incidents' are more serious in nature and has, or is likely to, result in a security breach which may compromise the confidentiality, integrity and / or availability of Council information, systems and assets.

Examples of calls that may typically be classified as event include:

- Council staff sharing ICT credentials - user name, password, system access.
- Internal communication error - email sent to the wrong Department or officer.
- Loss of an encrypted laptop containing personal data.

Examples of calls that may typically be classified as incident include:

- External communication error - letter or email sent to the wrong recipient that contains personal information.
- Inappropriate disclosure of personal information - i.e. erroneous posting of information on Council website or within a global communication.
- Loss of a hard copy paper file containing personal information.
- A virus that has penetrated the Councils network.

In determining whether a call should be dealt with as an incident or an event, the Information Management Team shall consider:

- ➢ Whether a breach has actually occurred (or whether there is potential for a breach to occur should preventative measure not be taken to mitigate risk),

- The sensitivity of the information,
- The number of data subjects affected,
- The potential impact on the data subjects affected,
- The potential impact on the Council,
- The action taken to contain / recover from the situation,
- In the case of loss or theft of personal / commercially sensitive information whether the data was encrypted.
- In the case of inappropriate disclosure of information, whether the disclosure was internal (e.g. between Council employees) or an external third party (e.g. member of the public).

Where there is uncertainty as to whether a call should be dealt with as an incident or an event, the Information Management Team will refer the matter to the IM Management Team for a decision.

2. Dealing with an information security 'event'

Information security events will be referred to, and dealt with by the relevant service areas Information Management Champion, in conjunction with the Line Manager.

Appendix I provides a process flow diagram illustrating the process that must be followed when investigating an event.

An up to date list of Information Management Champions can be found on Inform under the Support Services > Information Management > 'Contact Us' section.

3. Dealing with an information security 'incident'

All incidents will be fully investigated in order to establish the facts and any corrective and/or preventative actions required. Not all incidents will need the same depth of investigation to find out the full facts and determine what went wrong.

The incident investigation is intended to:

- Establish the facts - extent of the breach, amount of information involved, sensitivity of the information involved
- Determine what went wrong

- Identify the severity and potential impact on the Council and those involved
- Identify any potential for loss or damage to individuals, the Council or any other body
- Identify risks that are appropriate for follow up and action
- Make recommendations to address identified risks
- Inform future business processes and planning
- Whether to report the incident to the Information Commissioner (if it involves personal data) and or any other regulatory body

The incident investigation process will be lead by the Information Management Team in conjunction with the nominated service lead (Senior Officer / Manager) and the Information Management Champion.

Depending on the nature and severity of the incident the investigation may involve:

- Collecting and recording of evidence,
- Meeting with those involved,
- Taking statements, formal or informal, from those involved including any witnesses,
- Consulting/engaging the Council's Human Resources, Internal Audit and/or Legal Services Department,
- Reporting the incident to the Information Commissioner's Office where a 'serious breach' has been identified,
- Involving the Council's Press Team where the incident has or is likely to be made public.

Appendix II provides a process flow diagram illustrating the process that must be followed when investigating an 'incident'.

4. Actions / recommendations identified during an investigation

Following conclusion of an incident investigation, actions/recommendations are likely to be identified to mitigate the risk, as far as possible, of an incident of a similar nature happening again in the future. Actions/recommendations will be recorded on the incident investigation report.

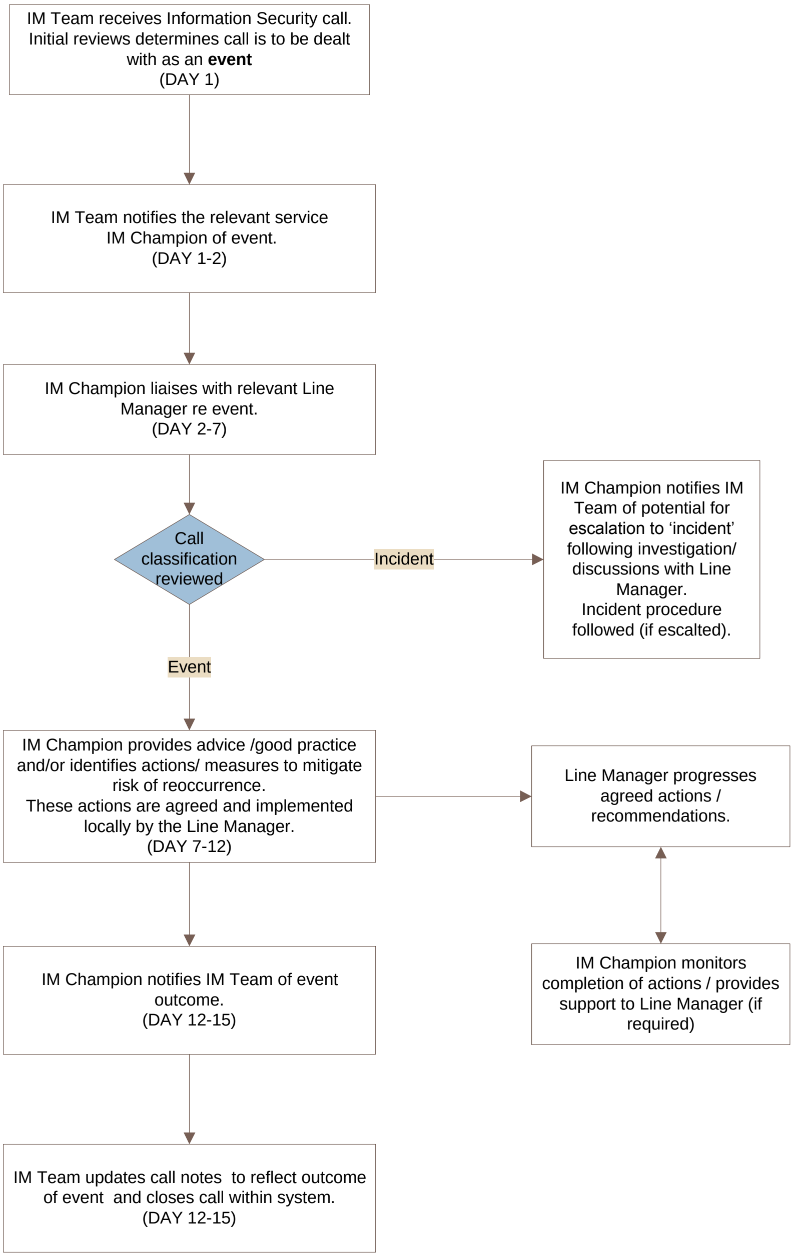
Each action will be given a due date for completion and will be assigned to a responsible officer. The responsible officer will be asked to sign the report confirming that the actions will be completed within the given timeframe.

It is the responsibility of that officer to ensure that all actions are completed in line with the investigation report and within the due date

In order to ensure that all actions are completed timely, a monitoring report identifying each action and their status will be sent to the accountable officer on a monthly basis for completion until all remedial actions are closed.

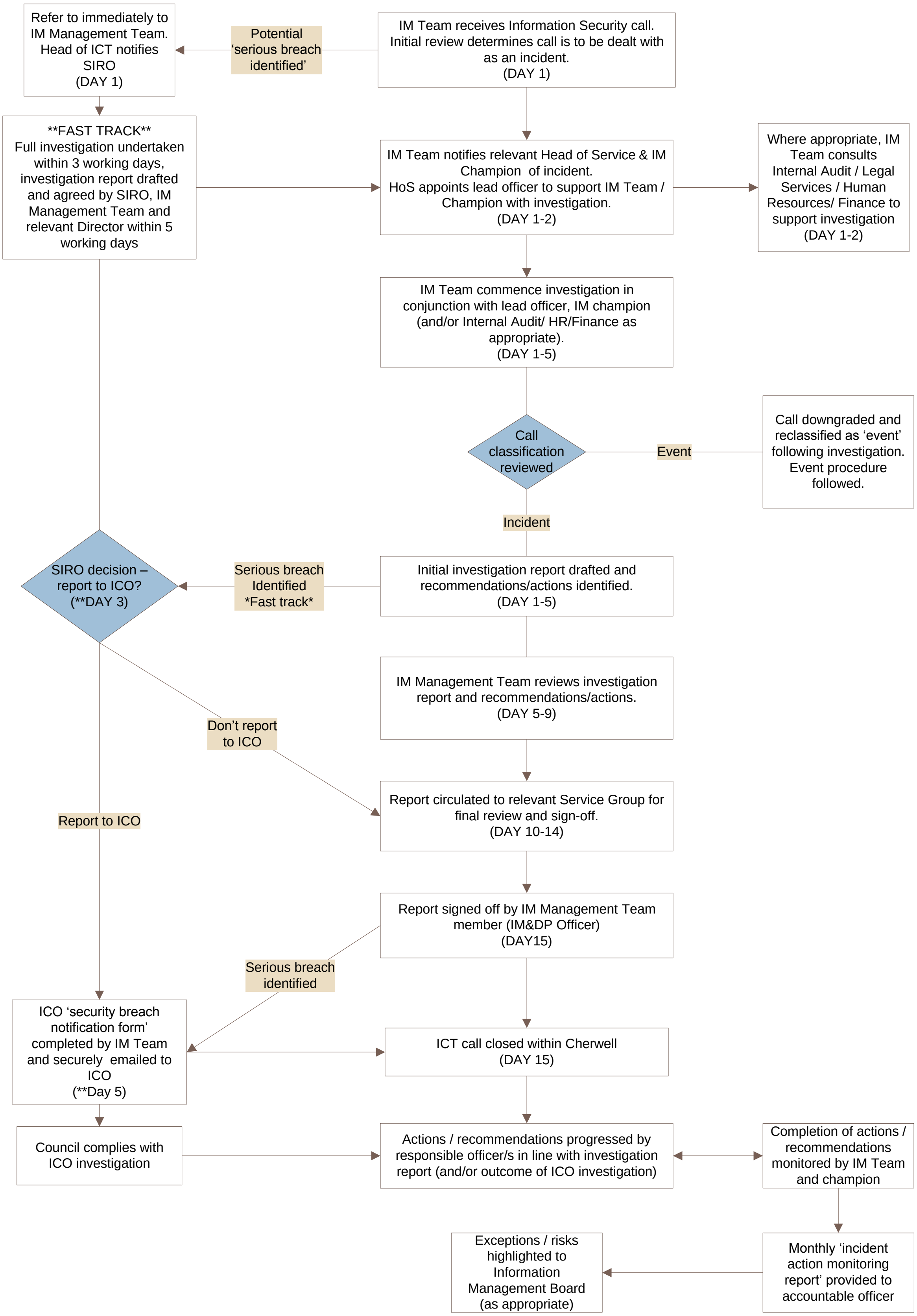
Any exceptions or risks may be highlighted to the Information Management Board for review.

Appendix I: Procedure for investigating an information security 'event'


IM Team receives Information Security call. Initial reviews determines call is to be dealt with as an **event** (DAY 1)
IM Team notifies the relevant service IM Champion of event. (DAY 1-2)
IM Champion liaises with relevant Line Manager re event. (DAY 2-7)
Call classification reviewed
Incident
IM Champion notifies IM Team of potential for escalation to ‘incident’ following investigation/ discussions with Line Manager. Incident procedure followed (if escalted).
Event
IM Champion provides advice /good practice and/or identifies actions/ measures to mitigate risk of reoccurrence. These actions are agreed and implemented locally by the Line Manager. (DAY 7-12)
Line Manager progresses agreed actions / recommendations.
IM Champion monitors completion of actions / provides support to Line Manager (if required)
IM Champion notifies IM Team of event outcome. (DAY 12-15)
IM Team updates call notes to reflect outcome of event and closes call within system. (DAY 12-15)

1 Day = 1 Working Day

Appendix II: Procedure for investigating an information security 'incident'



IM Team receives Information Security call. Initial review determines call is to be dealt with as an incident. (DAY 1)

Potential 'serious breach identified'

Refer to immediately to IM Management Team. Head of ICT notifies SIRO (DAY 1)

FAST TRACK Full investigation undertaken within 3 working days, investigation report drafted and agreed by SIRO, IM Management Team and relevant Director within 5 working days

IM Team notifies relevant Head of Service & IM Champion of incident. HoS appoints lead officer to support IM Team / Champion with investigation. (DAY 1-2)

Where appropriate, IM Team consults Internal Audit / Legal Services / Human Resources/ Finance to support investigation (DAY 1-2)

IM Team commence investigation in conjunction with lead officer, IM champion (and/or Internal Audit/ HR/Finance as appropriate). (DAY 1-5)

Call classification reviewed

Event

Call downgraded and reclassified as 'event' following investigation. Event procedure followed.

Incident

Initial investigation report drafted and recommendations/actions identified. (DAY 1-5)

Serious breach Identified *Fast track*

SIRO decision – report to ICO? (**DAY 3)

Don't report to ICO

Report to ICO

IM Management Team reviews investigation report and recommendations/actions. (DAY 5-9)

Report circulated to relevant Service Group for final review and sign-off. (DAY 10-14)

Report signed off by IM Management Team member (IM&DP Officer) (DAY15)

Serious breach identified

ICO 'security breach notification form' completed by IM Team and securely emailed to ICO (**Day 5)

ICT call closed within Cherwell (DAY 15)

Council complies with ICO investigation

Actions / recommendations progressed by responsible officer/s in line with investigation report (and/or outcome of ICO investigation)

Completion of actions / recommendations monitored by IM Team and champion

Monthly 'incident action monitoring report' provided to accountable officer

Exceptions / risks highlighted to Information Management Board (as appropriate)

Version Control

Version No	Date approved by IM Operational Group	Valid from	Valid to	Changes Made
1.0	10.08.2016	10.08.2016		New procedure developed based on former Information Incident Investigation policy.