STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**Managing Security Events and Weaknesses**
Effective Date:	**24 Apr 2019**
Reference Number:	**SOP-02-03**
Version Number:	**2.7**
Owner:	**Event and Incident Management Process Owner,**
Review Date:	**15 Aug 2020**

UNCONTROLLED IF STORED LOCALLY OR PRINTED

Table of Contents

UNCONTROLLED IF STORED LOCALLY OR PRINTED

1. Purpose

Information security events should be assessed and it should be decided if they are to be classified as information security incidents and these should be responded to in accordance with the documented procedures. Responsibilities and procedures should be established to ensure a quick, effective and orderly response to any information security incidents.

The purpose of this document is to describe the procedure to be followed when dealing with any identified security events, weaknesses and opportunities. It includes the process for classifying security events as incidents and the actions necessary to respond to these security incidents.

2. Scope

All security events, weaknesses and opportunities identified for the ISMS are in scope of this procedure.

3. Responsibilities

The Incident Management Team is responsible for:

- Dealing with security events including:
    - Completing the assessment stage for all reported items.
    - Notifying any managers assigned a stage action and advising on the management process
    - Managing data protection incidents
    - Reviewing if action stages have been completed and closing the record

The ISMS Improvement Team is responsible for:

- Dealing with weaknesses and opportunities including:
    - Completing the assessment stage for all reported items.
    - Notifying any managers assigned a stage action and advising on the management process
    - Reviewing if action stages have been completed and closing the record

The Information Security Manager is responsible for:

- Reporting corrective actions to the ISSG

The Information Security Steering Group (ISSG) is responsible for:

- Reviewing if corrective actions have been successful.
- Requesting internal audits or additional ISMS training for staff.
- Handling serious security events raised directly to them rather than through Q-Pulse

The Senior Information Risk Owner (SIRO) is responsible for:

- Handling serious security events raised directly to them rather than through Q-Pulse

The ISMS Management Sponsor and Head of Operations ISMS are responsible for:

- Performing the initial assessment when all members of the Incident Management Team are unavailable

UNCONTROLLED IF STORED LOCALLY OR PRINTED

4. Procedure

4.1. Reporting Security Events, Weaknesses and Opportunities

Security events, weaknesses and opportunities may be reported by any member of staff, contractor, visitor or user of the TRE and associated services. These will be created directly in Q-Pulse or added to Q-Pulse by the ISM (see SOP-02-02) and will first generate an assessment stage.

4.2. Serious Security Events

SOP-02-02 allows for serious security events to be raised directly with a member of the ISSG or the SIRO. In this situation the member of the ISSG or the SIRO to who the event was reported is responsible for the handling of the incident and the triage process described below does not apply.

4.3. Assessment Stage

Security events will be directed to the Incident Management team for assessment. Weaknesses and Opportunities will be directed to the ISMS Improvement Team for assessment.

During the assessment stage the responsible team will review the details of the item raised and perform an initial evaluation to confirm that the details have been recorded clearly and that the item has been correctly classified (e.g. as a security event). This will also determine whether an event should be classified as a security incident (see appendix for assessment criteria).

The responsible team (following any re-classification) will assign the remaining action stages for the management of the item to a responsible manager. This will usually be the process owner of the associated process. The responsible team will also review the target dates for completion of the action stages.
As part of the assessment stage additional action management stages may be added or removed from the item.
The stages available include:

- Assessment (already present in record)
- Containment
- Corrective action (already present for security event record)
- Dataset ethics consulted
- Effectiveness Check
- Investigation (already present for security event record)
- Report to IG SIRI?
- Review (already present for weakness and opportunity record)
- Root cause

Any fields relevant to the classification of the item e.g. Process, Event Category, Document, etc. will also be reviewed and updated as appropriate.

The following working days (after raised date) for completion of the default stages will be applied. Data protection security incidents are subject to external reporting controls (see section 4.3) and are not included in this table.

UNCONTROLLED IF STORED LOCALLY OR PRINTED

Item	Assessment	Investigation	Review	Corrective Actions
Security Incident (non data)	1	2	N/A	20
Security Event	1	7	N/A	30
Weakness or Opportunity	7	N/A	20	N/A

4.3.1. Triage rota for Incident Management

There is a rota which determines which member of the Incident Management Team is on-call and responsible for performing the initial assessment for each day of the week Monday-Friday. It is expected that the on-call person will be able to respond to email alerts within 4 hours. If the on-call person is unable to do this (holiday, sickness, all day meetings) then it is their responsibility to arrange for another member of the Incident Management Team to provide cover. To provide suitable redundancy there will be a minimum of 3 members of the Incident Management Team.

4.3.2. Triage process for Assessing Security Events

The triage process for assessing security events is as follows:

1. When a security event is created in Q-Pulse, an automated email is sent to the Incident Management Team via chi-incidents@listserv.manchester.ac.uk.
2. The on-call person is responsible to perform the initial assessment as laid out in section 4.2 within 4 hours of the email being sent.
3. After completing the assessment stage the on-call person will “Reply to all” on the initial email alert, to inform the rest of the team that the event has been triaged.
4. If the event has not been assessed within 4 hours then the remaining members of the Incident Management Team, the ISMS Management Sponsor and the Head of Operations ISMS are responsible for performing the assessment.

4.3.3. Triage process for Assessing Weaknesses and Opportunities

There is no formal triage process for assessing weaknesses and opportunities. When a weakness or opportunity is created in Q-Pulse, an automated email is sent to the individual members of the ISMS Improvement Team who will aim to complete the assessment by the due date.

4.4. Managing Data Protection Incidents

For security events that are classified as data protection incidents there are a series of specific process steps that must be followed for managing the incident.

UNCONTROLLED IF STORED LOCALLY OR PRINTED

4.4.1. Data Protection Incident Process

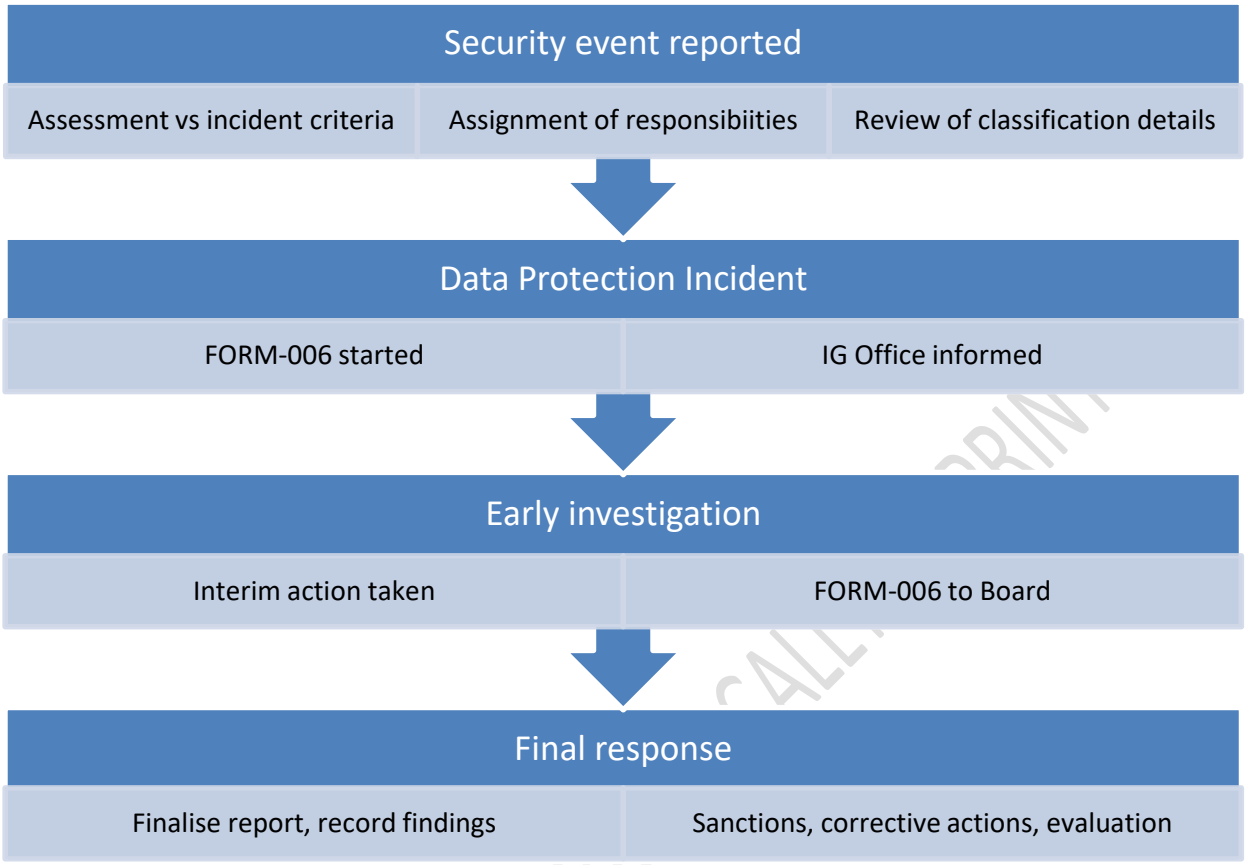

Figure 1: Flow diagram of the data protection incident process

Following the report of a data incident the Incident Management Team should:

- Gather preliminary information to determine the origin and nature of the incident in FORM-006 from the person who reported the incident and, if immediately available, colleagues involved or TRE system logs.
- Supply this gathered information immediately to the university Information Governance Office (IGO). They can instruct on how to proceed and advise on whether an IG SIRI has occurred. No-one should attempt to modify, limit or contain the extent of the incident unless explicitly instructed to do so by the IGO. Contact information is in the university's Information Security and Data Protection Incident Reporting SOP. The IG Office's level of involvement will depend on the nature of the incident, but expect initial containment within 4 hours, initial communications within 24 hours, further investigations within 72 hours, and further local advice on remedial actions within 5 days. *The IGO needs to be consulted for approval before the rest of this SOP is followed.*
- Swiftly stop access to any affected data and suspend any affected TRE accounts. If the incident could affect other TRE assets then all access to the TRE should be disabled.
- Gather further information about the suspected incident to complete an Incident Investigation Report (FORM-006).
- Take interim action as information about the incident becomes apparent, including contacting directly affected individuals (e.g. announcing that TRE access is suspended), notifying organisations contractually involved with the affected dataset, and imposing sanctions on anyone who broke rules.
- Circulate a Report (FORM-006) completed as far as possible to the next TRE ISMS Board detailing the nature of the incident, outcomes, and recommendations.

    - Share a redacted version of the report to other TRE users who request it. The redaction is to ensure anonymity of individuals involved and confidentiality of certain details about the TRE.
- Escalate and report via DSP Toolkit or other logging system as required.
- Ensure the incident and outcomes are correctly recorded in Q-Pulse
- Evaluate the incident response and update SOPs as appropriate once the incident is contained and the above actions have been completed.

4.4.1.1. Timeframes for Incident Communications

Notify key people about the incident in the following time frames:

- Initial findings and immediate actions by email to university IG Office and IG Manager (and to the wider management committee if the whole TRE is affected)<1 day
- In conjunction with the IG Office, notify the Information Commissioner's Office and the data controller if a statutory offence has occurred <3 days
- Thanks for reporting incident and advice (if appropriate) by email to person who reported incident <5 days
- Discussion of incident report by ISMS Board <2 weeks

4.4.1.2. Penalties, appeals, and accidents

For incidents where actions were accidental, such as spontaneous recognition of someone in a dataset, the TRE managers will enter into a dialogue with the affected TRE user and their line manager (or equivalent) to determine the best way to proceed.

Any TRE user who is found to have intentionally caused the incident will face the following sanctions:

- Formal warning
- TRE user account frozen until refresher training is completed
- Other sanctions mentioned in contracts relating to the TRE project

Where users acted maliciously or personal data is involved the following sanctions will be considered by TRE management:

- TRE user account frozen for a certain number of months and until refresher training is completed
- Refer to University (or notify user's host institution) for a research misconduct investigation, which can result in dismissal
- Refer to the ICO, which can result in fines and a prison sentence
- Other sanctions mentioned in contracts relating to the TRE project

Users can appeal against any imposed penalty by writing to the TRE Board within 4 weeks of the final report.

4.5. Ongoing Management of Security Events, Weaknesses and Opportunities

The process for the ongoing management of all items will be similar. The owner of each action stage is notified when the stage is assigned to them. They are then required to either: complete their actions by the target date; or reassign the stage to a more appropriate person. In the case of reassignment, the stage should be updated to explain why the change was made.

UNCONTROLLED IF STORED LOCALLY OR PRINTED

Each stage shall be completed with enough detail to allow an auditor to determine what happened and how it happened. If no action was taken, the stage owner shall record “no action taken” with a justification of why no action was taken.
Stages should be closed once all content is complete. Following the closure of all stages the owner of the final stage (normally ‘Corrective Action’ or ‘Review’) may also close the overall record. This action may also be completed by the Q-Pulse Administrator, members of the Incident Management Team (for Security Event and Incidents) or ISMS Improvement Team (for Weaknesses and Opportunities).

4.5.1. Escalation of Outstanding Action Stages

Stage owners will be prompted to complete outstanding action stages from 7 days prior to the target dates. Action stages that are not completed within 30 days after the target dates will be escalated to the stage owner’s line manager. Any activities still not completed within a further 15 days will be escalated to the ISMS Management Sponsor.

4.6. Follow-up and Reviewing Efficiency of Corrective Actions

When reviewing the efficiency of corrective actions, the Incident Management Team will liaise with the most relevant TRE staff members; this may include staff who reported the security event, staff who caused the security event, the line manager of the area where the security event was reported and customers that might have been affected by the security event. They may also look at the turnaround time and resources required for each stage and the security event as a whole.
The ISM will report the findings to the ISSG.
The ISSG will review the efficiency of the corrective action. Should this be found to be insufficient, the ISSG can make internal audit requests or may request additional training for associated staff.

5. Cross-referenced ISMS Documents

Number	Type	Title
FORM-006	ISMS\Forms	TRE Incident Investigation Report
SOP-02-02	ISMS\SOP\ISMS Management - SOP	Reporting Security Events
ISMS-04-01	ISMS\Policy & Guidance\ISMS Improvement - policy & guidance	ISMS Management Review
SOP-04-05	ISMS\SOP\ISMS Improvement - SOP	ISMS Internal Auditing

6. Appendices

6.1. Assessment Criteria for Escalation of Security Events

6.1.1. Definition of a Data Protection Incident

A data protection incident is an event or occurrence that has resulted or could have resulted in the disclosure of confidential information to an unauthorised individual, put at risk the integrity of the system, put at risk the availability of the services, or breached the Data Protection Act.

UNCONTROLLED IF STORED LOCALLY OR PRINTED

6.1.2. Definition of an IG SIRI

An IG Serious Incident Requiring Investigation (SIRI) is any incident which involves actual or potential failure to meet the requirements of the Data Protection Act and/or the Common Law Duty of Confidentiality. This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy.

Since June 2013 all organisations processing health and adult social care personal data should use the DSP Toolkit Incident Reporting Tool to report level 2 IG Serious Incidents Requiring Investigation (SIRI) to the Department of Health (DH), NHS England and the Information Commissioner's Office (ICO). Because the TRE falls under the University of Manchester's ICO registration, decisions around whether an incident constitutes an IG SIRI must be made in conjunction with the University's Information Governance Office.

There is no simple definition of a serious incident. What may at first appear to be of minor importance may, on further investigation, be found to be serious and vice versa. As a guide, an IG SIRI includes:

- Any incident which involves actual or potential failure to meet the requirements of the Data Protection Act
- Unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy and/or the Common Law of Confidentiality.
- Personal data breaches which could lead to identity fraud or have other significant impact on individuals.

UNCONTROLLED IF STORED LOCALLY OR PRINTED

6.1.3. Definition of Other Security Incidents

If a security event is not immediately identified as a data protection incident the following criteria should be used to assess the event. Where an event scores 2 or more for Confidentiality or 3 or more for Integrity, Availability or Additional Measures it should be classified as a security incident.

Value	Confidentiality	Integrity	Availability	Additional Value Measures (can be applied across all of the criteria)
1	- No impact on data confidentiality	- No impact on data accuracy or consistency - Any corruption or loss of data would not impact operations	- Loss of availability of this asset would not impact normal operations - Asset can be quickly restored within 4 hours	- Small number of individual correspondence/ representations - No measurable impact on research activity within specific teams - No impact on research income - Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of less than £100K - Technical breaches which may result in complaints to the University but complainant does not resort to legal action or regulatory referral - Breach results in minimal or no damage or loss
2	- Minor impact on data confidentiality (e.g. small subset of non-traceable data released) - Disclosure of the information would cause only minor embarrassment or minor operational inconvenience	- Minor impact on data accuracy or consistency but does not affect collaborators - Any corruption or loss of data is retrievable with minimal effort	- Temporary loss of availability would have a minor impact on normal operations - Asset can be restored within 1 day	- Reputation is minimally affected with little or no targeted effort or expense required to recover; - Small impact on research activity within specific teams - Mild stakeholder correspondence/ representations - Minor impact on research income or productivity for wider group - Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of between £100K- £500K - Fines or claims brought of less than £50K - Regulatory action unlikely or of only localised effect. - Advisory/improvement notices

UNCONTROLLED IF STORED LOCALLY OR PRINTED

Value	Confidentiality	Integrity	Availability	Additional Value Measures (can be applied across all of the criteria)
3	- Moderate impact on data confidentiality - Disclosure of the information would cause some reputational damage and has a short-term impact on operations	- Data corruption or loss has a noticeable impact on collaborators - Corruption requires resources and time to resolve	- Loss of availability of this asset would impact normal operations and prevent collaborators from accessing our services or data - Asset and availability can be restored within 2 days	- Reputation is damaged in the short to medium term with targeted effort and expense required to recover. - Public stakeholder comment and correspondence expressing concern - Low key local or regional interest media coverage - Medium term effect on productivity within discipline - Up to 1% overall reduction in research income due to loss of confidence/lack of compliance - Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of between £500K-£1M - Fines or claims brought of between £50K-£250K - Case referred by complainant to regulatory authorities who may request information or records as a result - Enforcement action notices.

UNCONTROLLED IF STORED LOCALLY OR PRINTED

Value	Confidentiality	Integrity	Availability	Additional Value Measures (can be applied across all of the criteria)
4	- Significant proportion of the data is accessible or released - Disclosure of the information has a significant impact on operations or tactical objectives	- Corruption or loss of data/asset would restrict operations and cause loss of collaborator confidence - Corruption requires significant resources and time to resolve	- Loss of availability of this asset would affect several processes and would prevent collaborators from accessing our services or data - Availability cannot be restored within 3 days and requires specific skills/personnel or significant resources	- Significant public and private comment from stakeholders expressing serious concerns - Adverse regional or national interest media coverage - Medium to long term effect on productivity in more than one discipline - 1 to 4% overall reduction in research income due to loss of confidence/lack of compliance - Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of between £1M-£2.5M - Fines or claims brought of more than £250K - Incident requires escalation to UoM Data Protection Officer or IG SIRI - University required to report serious matter to regulators - Case referred by complainant to regulatory authorities and potential for regulatory action with more than localised effect

UNCONTROLLED IF STORED LOCALLY OR PRINTED

Value	Confidentiality	Integrity	Availability	Additional Value Measures (can be applied across all of the criteria)
5	- All of the data is accessible or released - Disclosure of the information has a serious impact on long term strategic objectives or puts the survival of the organization at risk.	- Corruption or loss of data halts all operations and would cause major loss of collaborator confidence. - Corruption requires extensive resources and time to resolve	- Loss of this asset would prevent the TRE from operating and providing any of its services to its collaborators - Availability cannot be restored within 5 days and requires specific skills/personnel or significant resources	- Reputation damaged for the long term or irrevocably destroyed - Adverse high profile, national media coverage from reputable/ influential media, with some international interest - More than 5% reduction in research income due to loss of confidence/lack of compliance - Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of greater than £2.5M - Incident requires escalation to UoM Data Protection Officer or IG SIRI - Formal external regulatory investigation into organisational practices with potential for suspension of significant elements of University operations - Withdrawal of status or imposition of sanctions resulting in forced termination of mission critical activities

UNCONTROLLED IF STORED LOCALLY OR PRINTED