



STANDARD OPERATING PROCEDURE

Do not Photocopy

Document Information Classification: Unrestricted

Title:	Reporting Security Events
Effective Date:	24 Apr 2019
Reference Number:	SOP-02-02
Version Number:	2.3
Owner:	Event and Incident Management Process Owner,
Review Date:	04 Apr 2020

Table of Contents

1. Purpose	3
2. Scope	3
3. Responsibilities.....	3
4. Procedure.....	3
4.1. Personnel Without Access to Q-Pulse.....	4
4.1.1. Reporting Security Events	4
4.1.2. Reporting a Serious Security Event	4
4.1.3. Reporting a Security Weaknesses or Opportunity	4
4.2. Personnel With Access to Q-Pulse	5
4.2.1. Reporting a Security Event Using the Q-Pulse Web Interface	5
4.2.2. Reporting a Security Event Using the Q-Pulse Windows Client.....	6
4.2.3. Reporting a Security Weakness or Opportunity	9
4.2.3.1. Using the Q-Pulse Web Interface	9
4.2.3.2. Using the Q-Pulse Windows Client.....	10
4.3. Additional steps required by University of Manchester Policy.....	11
5. Cross-referenced ISMS Documents	12
6. Appendices.....	12

1. Purpose

Procedures must be established for the reporting of information security events and all employees should be made aware of their responsibility to report information security events as quickly as possible. Employees should also be required to note and report any observed or suspected information security weaknesses and opportunities for improvement in systems or services.

This document describes the procedure for reporting information security events, weaknesses and opportunities.

2. Scope

The reporting of all security events, weaknesses and opportunities for all employees.

The management of reported security events, weaknesses and opportunities, including assessment and further response is out of scope of this procedure.

3. Responsibilities

All CHI staff and students

- Reporting security events, weaknesses and opportunities via the defined mechanisms

The Information Security Steering Group (ISSG) and the SIRO (Senior Information Risk Owner)

- Responding appropriately to serious events raised directly to them

4. Procedure

Situations to be considered for information security event reporting include:

- Ineffective security control;
- Breach of information integrity, confidentiality or availability expectations;
- Human errors;
- Non-compliances with policies or guidelines;
- Breaches of physical security arrangements;
- Uncontrolled system changes;
- Malfunctions of software or hardware;
- Access violations.

Malfunctions or other anomalous system behavior may be an indicator of a security attack or actual security breach and should therefore always be reported as an information security event.

Examples might include:

- Unauthorized access to the building or data
- Removal of data or sensitive information from TRE
- Actions that risk the disclosure of sensitive information, e.g. not using encryption when sending data via email, unsecure storage of information, copying data to public computers
- Disclosure of passwords or alarm codes
- Attacks on the network
- Failure of utilities, e.g. electrical supply
- Theft of hardware, information or paperwork

- Loss or corruption of data

Security weaknesses and opportunities are where there are observed or suspected issues with the existing systems or processes. Note: Staff should not try to prove any suspected security weaknesses as this could result in damage to the service and result in a real security incident.

4.1. Personnel Without Access to Q-Pulse

4.1.1. Reporting Security Events

Personnel without access to Q-Pulse should report security events to the ISM via email to: chi-incidents@listserv.manchester.ac.uk.

The email should include:

- Date (and, if possible, time) of security event.
- Detail of the event.
- Action Taken (where appropriate):
- Name of Person reporting the event.

An example is shown below:

Date and Time: dd mmm yy hh:mm
 Detail of Event: Swipe card was found outside main entrance to Vaughan House. No observed breach of security.
 Action Taken Card returned to Operations Team.

 Raised by (Name)

4.1.2. Reporting a Serious Security Event

It is also possible to report a serious security event verbally direct to a member of the ISSG or the SIRO. This would be for events where the reporting person considered that immediate action was required. The event should then be raised in Q-Pulse as per 4.1.1 as soon as possible.

4.1.3. Reporting a Security Weaknesses or Opportunity

Personnel without access to Q-Pulse should report security weaknesses and opportunities to the ISM via email to: chi-incidents@listserv.manchester.ac.uk.

The email should include:

- Detail of the observed or suspected weakness or opportunity.
- The Process that is affected (if known)
- Name of Person reporting the proposal.

An example is shown below:

Weakness: The main door to Vaughan House shuts very slowly and could allow tailgating of unauthorised visitors.
 Process: TRE Physical Security

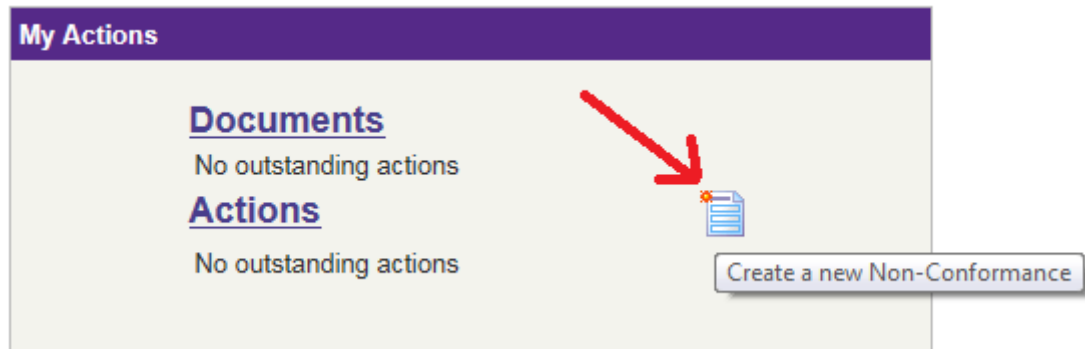
 Raised by (Name)

4.2. Personnel With Access to Q-Pulse

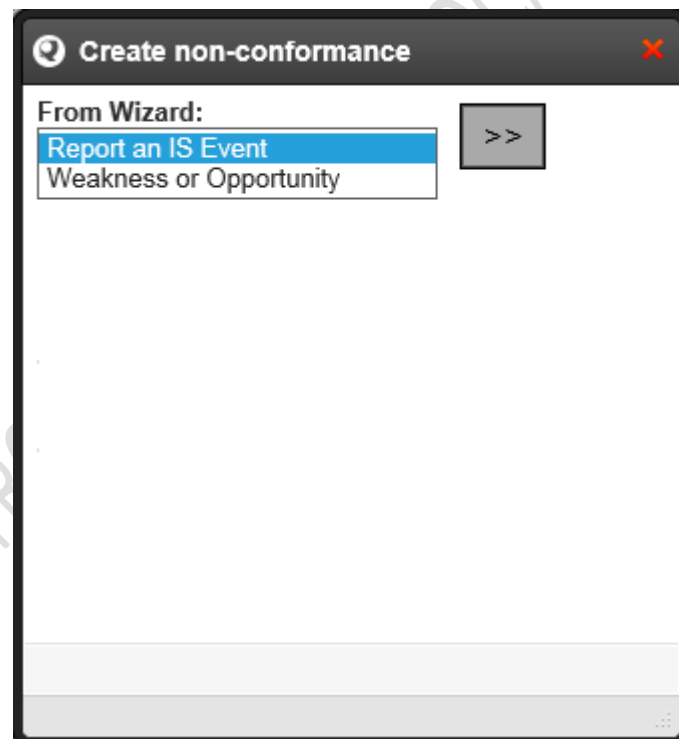
All staff with Q-Pulse accounts will have access to event reporting.

4.2.1. Reporting a Security Event Using the Q-Pulse Web Interface

From the 'My Actions' Launchpad click on the icon to 'Create a new Non-Conformance'.



From the 'Create non-conformance' dialog select the wizard for reporting an IS Event



This will display the screen for entering the details of the information security event.

Report an IS Event Wizard

Information Security Event


Details *

Attachment

Event Category *

Any

Raised By Person *



Source *

Event


Please click Finish to notify the ISM who will complete an assessment of the security event.

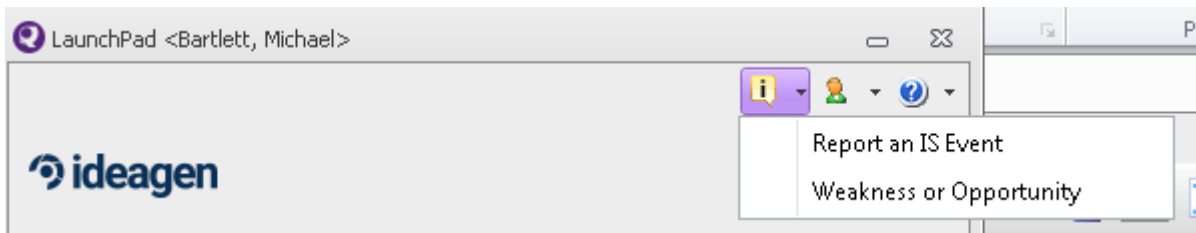
Complete the fields for the information security event as follows:

- **Details** – Enter the details of the event. Include the date and time observed if possible.
- **Attachment** – Attach any documents that may support or assist the event report.
- **Event Category** – Where possible select an item from the drop-down to classify the nature of the security event e.g. malfunction of hardware, non-compliance.
- **Raised by Person** – Add the name of the person that is reporting the event
- **Source** – This field is set by default to “Security Event” and **should not be updated**.

When all of the necessary information has been added, click on ‘Finish’ to submit the details of the security event to the ISM. The information entered will be used to assess the event and assign it to an appropriate owner for further action.

4.2.2. Reporting a Security Event Using the Q-Pulse Windows Client

To raise an incident via the Q-Pulse Windows client, click on the ‘Ideas’ dropdown  on the toolbar of the Launchpad and select ‘Report an IS Event’.



Note: If the wizard does not appear see SOP-02-06 for details of how to add the wizard to your Launchpad.

The “Welcome” screen will be displayed. Click on ‘Next’ to continue.



Report an IS Event Wizard

Information Security Event
Please enter the details of the event and attach any evidence if available. If possible please also include the date and time the event was witnessed.

Details

Attachment

Event Category

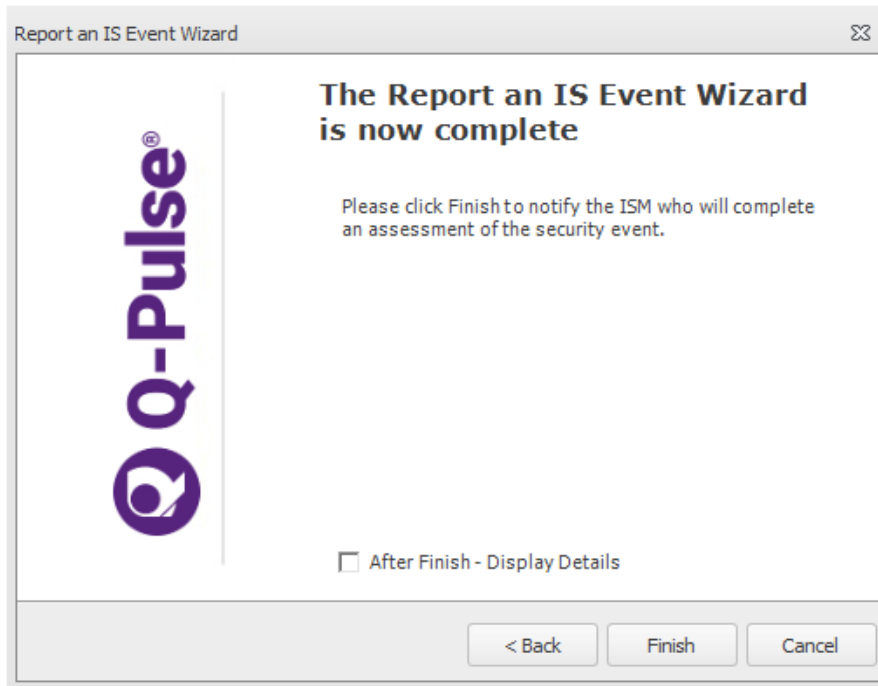
Raised By Person

< Back Next > Cancel

Complete the fields for the information security event as follows:

- **Details** – Enter the details of the event. Include the date and time observed if possible.
- **Attachment** – Attach any documents that may support or assist the event report.
- **Event Category** – Where possible select an item from the drop-down to classify the nature of the security event e.g. malfunction of hardware, non-compliance.
- **Raised by Person** – Add the name of the person that is reporting the event
- **Source** – This field is set by default to “Security Event” and **should not be updated**. Note: It is only visible if the screen is scrolled.

When all of the necessary information has been added, click on ‘Next’ and the final screen will be presented.



Click on 'Finish' to submit the details of the security event to the ISM. The information entered will be used to assess the event and assign it to an appropriate owner for further action.

4.2.3. Reporting a Security Weakness or Opportunity

The Q-Pulse steps are similar for reporting a security weakness or opportunity although some of the fields that are required will differ. Only the data entry dialogs will be shown here.

4.2.3.1. Using the Q-Pulse Web Interface

The wizard screen will be presented in the web interface as follows:

Weakness or Opportunity Wizard

Weakness and Opportunities

Details *

Attachment

Process

Any

Raised By Person *



Source *

Opportunity

Please click Finish to notify the ISM who will complete a review of the proposal.

Complete the fields for the information security event as follows:

- **Details** – Enter the details of the weakness or opportunity.
- **Attachment** – Attach any documents that may support or assist the proposal.
- **Process** – Where possible select an item from the drop-down to classify the process that is affected by the proposal e.g. Staff Induction, Update and Exit.
- **Raised by Person** – Add the name of the person that is reporting the weakness or opportunity.
- **Source** – This field is set by default to “Opportunity” and **should not be updated**.

4.2.3.2. Using the Q-Pulse Windows Client

The wizard screen will be presented in the windows client as follows

Complete the fields for the information security event as follows:

- **Details** – Enter the details of the weakness or opportunity.
- **Attachment** – Attach any documents that may support or assist the proposal.
- **Process** – Where possible select an item from the drop-down to classify the process that is affected by the proposal e.g. Staff Induction, Update and Exit.
- **Raised by Person** – Add the name of the person that is reporting the weakness or opportunity.
- **Source** – This field is set by default to “Opportunity” and **should not be updated**. Note: It is only visible if the screen is scrolled.

4.3. Additional steps required by University of Manchester Policy

In addition to the above steps, it may be necessary to report the event to the following groups. If in doubt - report it.

Theft or loss of university data or equipment, regardless of where the data/equipment was taken from, should be reported to the university security office on 0161 306 9966. The security office will contact you to discuss the type of data that has been lost or stolen and to determine the action to be taken. The security office is also the first point of contact when stolen property is found, and so they should have a full record of the event.

Personal data at risk events should be reported to the Records Management Office on 0161 275 8111, or outside of office hours via email to: infosec@listserv.manchester.ac.uk. The Records management office will provide advice and guidance on the next steps; they may also decide to contact the Information Commissioner’s Office.

For any event where you feel appropriate action is not being taken then it may be escalated to the University Information Security Manager on 0161 275 2122.

5. Cross-referenced ISMS Documents

Number	Type	Title
SOP-02-06	ISMS\SOP\ISMS Management - SOP	Use of Q-Pulse
SOP-02-03	ISMS\SOP\ISMS Management - SOP	Managing Security Events and Weaknesses
SOP-03-11	ISMS\SOP\TRE Operations - SOP	Protecting the TRE from Malware

6. Appendices

None