Title:	Information Security Incident Management		
Version:	1.2	Effective Date	June 2018
Summary	Description of the procedure for managing information security incidents, including data protection and cyber security incidents, for use by those involved in the procedure		

Ensure that you are using the most up to date version of this document by checking the University's online document system https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=37622

1 Background and Purpose

The University has implemented a number of technical and procedural controls, including two-factor authentication, and staff training to help protect the University's information from a breach affecting its confidentiality, integrity, availability and/or authentication systems. Where these measures fail, either deliberately or accidentally, this procedure must be followed.

The purpose of this Procedure is to ensure that all actual and potential information security incidents are effectively managed in order to:

- facilitate a fast response to incidents in order to contain or minimise:
  - the impact of the incident on individuals;
  - the University's exposure to financial loss, reputation damage legal matters and/or contractual impacts; and
  - the potential operational impact from any decisions by Government departments including the Information Commissioner's Office (ICO) who may suspend processing and/or information flows;
- clarify the roles and responsibilities of those involved in managing information security incidents;
- provide support to those interested parties who are affected by incidents, both internally and externally;
- facilitate the analysis of incidents for reporting to senior management;
- identify the causes of incidents so that lessons learnt/improvements can be made to mitigate the risk of further occurrences; and
- facilitate prompt reporting as necessary to the Office for Students, the Information Commissioner's Office and any other external third-parties.

2 Definitions and Scope

For the purposes of this Procedure the following definitions apply:

Information Security Incident ("Incident") – is an event or suspected event which results, or has the potential to result, in a breach affecting the confidentiality, integrity, availability and/or authenticity of information or information assets at or involving the University, including actual or suspected incidents. It includes any identified security weaknesses that may cause an incident to occur. It includes but is not limited to:

- Cyber Incidents – an incident that compromises the security of University IT systems e.g. hacking, denial of service, phishing emails, and malware; and
- Incidents involving Very Sensitive or Highly Restricted information - a breach of security leading to the accidental, unlawful or malicious destruction, loss, unauthorised alteration, unauthorised disclosure of, or access to, data transmitted, stored or otherwise processed.

3 Procedure and Responsibilities

3.1 Responsibilities

3.1.1 All incidents:

The Information Governance Office (IGO) is responsible for:

- providing initial, on-going and bespoke, training and awareness for the application of the information security incident management process across the University as required;
- ensuring all Incidents are recorded as per the Information Security and Data Protection Reporting Standard Operating Procedure ("SOP");
- co-ordinating a response to any Incident, including as appropriate, the following actions:
    - log (capture and record the time the incident was reported;
    - contain;
    - assess;
    - investigate;
    - eradicate/recover; and
    - follow up/lessons learned;
- ensuring an appropriate incident response team is put in place;
- maintaining a record of incidents and investigations performed;
- reviewing and updating information security procedures and implementing changes to information security controls including physical security for offices, rooms and facilities to reflect findings from incident investigations;
- ensuring that corrective action is taken by the relevant process/information owners, information users or service providers; and
- retaining evidence of action taken.

3.1.2 Cyber incidents:

The IT Services Directorate (IT Services) is responsible for:

- taking any immediate and necessary steps to contain any cyber incidents;
- protecting/preserving the University's services in line with standard operating procedures; and
- protecting/preserving personal data and other information under the governance and control of IT Services.

IT Services should ensure that the IGO is informed of the cyber incident in accordance with the Information Security and Data Protection Incident Reporting SOP.

3.1.3 Personal data incidents:

The IGO is responsible for:

- considering whether a personal data breach has occurred;
- whether to take other mitigating actions; and
- obtaining evidence to enable the Data Protection Officer or certified deputy ("DPO"), in consultation with the Directorate of Legal Affairs, to decide whether or not to notify the ICO and/or inform the data subjects affected.

The DPO is responsible for notifying the ICO and/or data subjects where appropriate.

3.2 Procedure - Incident response – action and timescales

3.2.1 Triage - Immediate containment action and assessment (to be completed within 4 hours of the IGO being informed):

3.2.1.1 Once the incident is reported to the IGO it will be triaged in order to consider whether the reported event is an incident, to determine the impact severity (see Appendix 1) and any immediate containment action. This might include:

- contacting IT Services to request urgent action as appropriate if not already undertaken; and
- advising on urgent corrective action eg in relation to emails sent in error.

3.2.1.2 The IGO triage will obtain a detailed description of the Incident, including:

- nature of the information e.g. is it personal data or commercially sensitive information;
- data and volumes - request a copy of emails and files involved if not already provided;
- description of events and timings;
- determine if any related core business system owner has been informed e.g. where personal data information has been extracted from Campus Solutions, Resource Link or other core business systems;
- determine if anyone else has been informed such as the relevant Information Governance Guardian; and
- determine what, if any, mitigating actions have already been taken.

3.2.1.3 If the impact severity is "moderate" (see Appendix 1) or above, or if it is not possible to obtain sufficient information during the triage process, an Investigation Lead will be identified to investigate and determine if the assistance of the Information Security Incident Response Team (ISIRT) is needed (see 3.2.2.2) .

3.2.1.4 The IGO triage records the incident in OneTrust together with any correspondence related to the incident.

3.2.2 Incident response – for completion in the first 24 hours

3.2.2.1 Overarching Principles:

The Information Security Incident Response Plan may be initiated (see Appendix 3) where:

- the incident is already publically known;
- it has potentially major negative impact on the University or individuals;
- there is a wide-ranging impact on individuals or business operations; and/or
- wide-ranging involvement across the University is required to manage it.

The University's Major Incident Response Plan (MIRP) will supersede this process in the event of a major incident/crisis as defined in the MIRP.

3.2.2.2 Information Security Incident Response Team (ISIRT)

The ISIRT will:

- agree and take containment action if not already completed;
- determine next steps for further action and resources required; and
- agree communication plan to senior staff and timing.

The ISIRT comprises a core team with subject matter expert (SME) assistance added as and when required. The core ISIRT will comprise the following:

- Head of Information Security;
- Head of Data Protection;
- Records Manager;
- Information Governance Officer;
- IT security SME; and
- Data Protection SME.

Depending on the severity of the incident, membership of the ISIRT may additionally include:

- Head of Information Governance;
- DPO;
- University Solicitor;

- Communications SME;
- IT Risk Manager; and
- Head of Research Governance, Ethics and Integrity.

ISIRT roles/responsibilities:

- The Incident Controller will normally be the Head of Information Security or agreed alternative, and will allocate actions and decide the meeting frequency to manage the incident until an 'in control' state is achieved.
- The Investigation Lead will normally be an Information Governance Officer who will gather evidence of the incident and record all actions taken during the investigation in the Information Security Incident Management Report (Appendix 2) in order to enable the ISIRT to assess the severity of the incident.
- Where required, the ISIRT will ensure that:
    - the incident is reported to the appropriate internal or external body/organisation (e.g. ICO, NHS, funding bodies);
    - status updates are provided to senior staff; and
    - internal and external communications are approved.

3.2.2.3 Senior Staff:

Where appropriate a brief summary of the incident must be given to the following Senior Staff:

- Head of Information Governance;
- Senior Information Risk Owner;
- the Registrar, Secretary and Chief Operating Officer;
- Director of Legal Affairs and Board Secretariat;
- Director of Compliance and Risk;
- Director of Estates and Facilities;
- Director of IT Services (if IT involved); and
- Director of Communications and Marketing.

3.2.3 Within 48 hours of a personal data breach being reported to the IGO:

On the basis of available information, the DPO determines:

- whether or not the ICO is to be notified of the incident - notification is required unless the breach is unlikely to result in a risk to the rights and freedoms of individuals; and
- whether or not the affected individuals are informed of the incident – notification is required if/where the breach is likely to result in a **high** risk to an individual's rights and freedoms and should be done without undue delay.

Where the impact severity of the incident is "minor "(see Appendix 1), the DPO will contact the ICO/data subjects where required. If the impact severity is "moderate" and the DPO believes that the incident should be reported to the ICO and/or data subjects informed, they will advise Senior Staff (see 3.2.2.3) accordingly prior to reporting.

If the elapsed time is likely to exceed 72 hours between the University becoming aware of a breach and the conclusion of the investigation (eg due to weekends, University closure, absence of key people), the DPO will report the incident to the ICO, subject to further clarification once the investigation has concluded.

3.2.4 Within 72 hours – reportable personal data breach notified to ICO.

3.2.5 Within 5 working days (all Incidents):

- The Information Governance Guardian and/or Information Asset Owner assist(s) with local investigations and collaborate(s) with the ISIRT, to propose remedial actions, chasing responses as necessary.
- Head of Research Governance, Ethics and Integrity will consider the Incident in the light of any ethics application or sponsor agreements and recommends actions as appropriate.
- The IGO will review the incident handling process, summarise the action plan and ensure approval of conclusions and actions from Senior Staff (listed in paragraph 3.2.2.3) are obtained as necessary, recording all actions taken during the investigation in the Information Security Incident Management Report (Appendix 2).

3.2.6 Post-incident follow-up

The IGO will:

- finalise the Information Security Incident Management Report and ensure the report is retained for 3 years from the date the incident is reported to the IGO; any related correspondence (eg held locally) must be retained to the end of the academic year plus 1year;
- ensure that any agreed remedial actions are logged, together with agreed timescales for completion;
- ensure that the Incident Tracking Log is updated;
- liaise with Information Governance Guardians to ensure that local actions are completed;
- escalate any actions which have not been completed; and
- arrange updated guidance material to reflect any learning outcomes.

4 Reporting

The Head of Information Governance will provide a report on this Procedure to the Information Governance Committee. A summary report will be provided comprising:

- the number and type of incidents raised;
- incidents not reported to the IGO within 24 hours;
- reportable personal data breaches not communicated to the ICO within 72 hours;
- the key factors giving rise to the incidents and possible mitigation to prevent further occurrence; and
- any lessons learned to improve the Procedure.

Any significant incidents will be reported to IGC at their quarterly meetings.

5 Review of procedure

This Procedure will be reviewed at least every two years or when significant changes are required.

6 Contact list for queries related to this procedure

Role	Name	Telephone	email
Head of Information Governance	Tony Brown	0161 306 2106	Tony.brown@manchester.ac.uk
Head of Information Security	Eddie Hill		Eddie.Hill@manchester.ac.uk
Head of Data Protection	Callum Lyons		Callum.Lyons @manchester.ac.uk

Document Control

Procedure title:	Information Security Incident Management Standard Operating Procedure
Date Approved	June 2018
Approving Body	Information Governance Committee – minor changes approved by Head of IG
Version	1.2
Supersedes	Data Protection Incident Management SOP
Previous Review Dates	N/A
Next Review Date	June 2024
Related Statutes, Ordinances & General Regulations	
Related Policies	• Data Protection Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914 • Information Security Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525
Related Procedures	• Information Security and Data Protection Incident Reporting SOP: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=15678 • Information security classification, ownership and secure information handling SOP: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971 • Acceptable Use SOP for Staff: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221 • Acquisition, Development and Maintenance of IT Systems and/or Services SOP: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16369 • PCI DSS Incident Response Management SOP: http://documents.manchester.ac.uk/display.aspx?DocID=29831
Related guidance and or codes of practice:	• Information security classification examples - confidential information: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=15677 • NHS SIRI Guidance https://improvement.nhs.uk/resources/serious-incident-framework/ • ICO guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
Related Information	
Procedure Owner	Head of Information Governance

Version Amendment History

Version	Date	Reason for change
1.0	October 2017	Creation
1.1	June 2018	Clarification of types of incidents; specific changes in relation to personal data breaches and role of the DPO; added appendices for severity assessment and response plan; minor changes to wording and job titles; for approval by DPO and HOIG prior to circulation for comment; appendix 1 amended following input from IT Services
1.2	June 2022	Amended links; added Very Sensitive classification; updated contacts

Appendix 1 Impact severity assessment

DOMAINS	NEGLIBLE	MINOR	MODERATE	MAJOR	CATASTROPHIC
Risk to rights and freedoms of individuals	Potential for non-material damage to individuals; Low volume personal data (less than or equal to 5 data subjects); no special category data	Potential for physical or material damage to individuals; Several data subjects' personal data (over 5 but less than 300); low volume special category data (less than or equal to 5)	Potential for significant physical or material damage to individuals; High volume personal data (300 or more data subjects); special category data (more than 5 data subjects)	Death of an individual or significant damage to several individuals; Personal data of several thousand data subjects	Multiple major injuries or deaths; Personal data of millions of data subjects
Adverse University publicity/ reputation	No public impact;	Adverse publicity in local media; Adverse publicity in wider University	Adverse publicity in national media; Loss of confidence in University services	Major international adverse publicity; Total loss of public confidence	Governmental takeover/administration
Financial loss to University	No financial loss	Financial loss under £10M	Financial loss between £10M-£20M eg Withdrawal of one or more significant research grants or donations; significant financial loss due to premature disclosure of IP	Financial loss £20M - £100M	Financial loss >£100M
Disruption to business operations	Some delays or cost directly due to incident; Impacts up to 10 users	Reduced ability to make management decisions; Impacts between 10 and 100 users	Severe operational impact; Severely impaired ability to make management decisions; Loss of key controls; Key objectives/deliverables not met; Impacts between 100 and 500 users	Punitive regulatory consequences; Impacts more than 500 users;	Governmental takeover/administration

Appendix 2 INFORMATION SECURITY INCIDENT MANAGEMENT REPORT

To be updated as the incident investigation progresses and kept by the Information Governance Office as a record of how the incident was managed

Name of person initially reporting the incident	
Faculty/School/Unit	
Tel	
Date/time incident occurred or was discovered	
Date/time IG Office were informed of the incident and method of notification	
Information Owner	
IGO reference number	

1 Description of data lost, stolen, released or corrupted [include examples of type of data and volumes of records affected]

2 Circumstances of the loss, theft, release or corruption [include location, IT hardware and applications involved, who has been contacted in relation to the incident, timing of events, duration of exposure, evidence of access by unauthorised persons]

3 Immediate containment action [eg details of action taken to minimise/mitigate effect on data subjects (if relevant) and the University]

4 Risk assessment [consider confidentiality, integrity, availability and authentication risks; severity of the impact on individuals and/ or the University]

5 Whether any other regulatory body or collaborative partner has been informed and their response [eg Information Commissioner's Office, NHS partners] and DPO decision taken regarding ICO and/or data subjects notification where appropriate)

6 Log of actions taken during the investigation where a number of actions and/or people are involved (where copies of emails alone do not adequately track progress)

7 Communication of the incident within the University [eg to Senior Staff, to Information Governance Guardian, to Information Owner of any related core business system].

8 Short-term remedial action recommended to prevent a further occurrence [include name of action owner and target dates for completion where appropriate]		
Action	Owner	Target date

9 Longer-term remedial action recommended to prevent a further occurrence and wider issues identified *[include name of action owner and target dates for completion where appropriate]*		
Action	Owner	Target date

10 Review of incident handling [what could be improved eg communication, speed of response]

Appendix 3 - Information Security Incident Response Plan

1 Summary

A formal Information Security Incident Response Team (ISIRT) and the Information Security Incident Response Plan will be initiated when an incident meets some or all of the criteria described below:

- The incident is already publically known
- It has potentially major negative impact on the University or individuals
- There is a wide ranging impact on individuals or business operations
- Wide ranging involvement across the University is required to manage it

How the Response Plan is carried out is described below:

1.1 The Head of Information Security (or member of IGO as agreed) should assume the role of Incident Controller.

1.2 In consultation with the Data Protection Officer (DPO), assess whether the incident is a personal data breach and needs to be reported to the ICO, and/or the Data Subject(s)

If Yes, the DPO should action this.

1.3 Establish team membership appropriate to the incident.

1.4 Convene a meeting of the ISIRT.

1.5 Identify and requisition a "war room" if necessary. Dial-in facilities may be useful if key members are unable to be present.

1.6 The Incident Controller should start the meeting by assigning a scribe, who will normally be the relevant Information Governance Officer.

- The 20 Minute Meeting Agenda (see section 2) should be used for the initial meeting.
- The strategic objectives relating to the incident should be reviewed at the start of the meeting using the Strategy Statement (see section 3). Strategic priorities may vary at different times of the academic calendar.
- The scribe should use the 3IA template (see section 4) to record all relevant information, Issues, Ideas and Actions.

1.7 A Situation Report (see section 5) should be issued asap to the agreed stakeholders. Further SITREPs should be released on a regular basis with realistic intervals for progress.

1.8 The ISIRT should continue to meet at regular intervals until the response is normalised and agreed as per the Information Security Incident Management SOP.

2 Meeting Agenda (20 min version)

Date:…… Time:…… Location:…… Names of those present and departments represented:

No	Minutes	Item	Presented by	Resultant action and timeframe
1	2	Situational Overview Summary or update	ISIRT Chair or temporary leader or subject matter expert (SME)	
2	1	Indication of key strategy objectives direction	ISIRT Chair or temporary leader or subject matter expert (SME)	
3	2	All business units consider issues and ideas for action	This is done in silence	
4	10	Business units report for 1 minute each on the	Business unit representatives.	

No	Minutes	Item	Presented by	Resultant action and timeframe

		• Issues affecting
		  ○ people
		  ○ systems
		  ○ premises
		  ○ business
		  ○ reputation
		• intentions
		  ○ 0-24 hours
		  ○ 24 hours plus
		• any required help
		• any escalation for direction
		• any likely PR issues
		• who you will need discussions with afterwards
			This is high level and is not a debate, it is heard in silence by the rest.	

5	3	Direction for business units	ISIRT Chair	
6	2	AOB and set next meeting time	ISIRT Chair et al	

3 Strategy Statement [to be agreed]

Objectives	Enabling Activities	Target Date/Time	Remarks (Responsible/Resources)
1. Minimise harm and distress to individuals	1.1		
	1.2		
	1.3		
2. Protect the reputation of the University	2.1		
	2.2		
	2.3		
3.Minimise financial loss to the University	3.1		
	3.2		
	3.3		
4.Minimise disruption to business operations	4.1		
	4.2		
	4.3		

4 3IA Template

Information	Issues	Ideas	Actions
The facts (not assumptions) of the problem/situation	Identify the issues arising/the effect of the situation	Identify different solutions to mitigate/resolve issues. Discuss/evaluate	Select the most effective action, implement and log

Information	Issues	Ideas	Actions

5 Situation Report (SITREP)

Date:…… Time:…… Name:…… Role:……
Location:……

1	Nature of SITREP circle as appropriate	Urgent	Routine Update	Other specify ……
2	What has happened , brief description of incident?			
3	What is the effect on the University or individuals?			
4	What are your intentions 0-24 hours?			
5	What direction do you require?			
6	What practical assistance do you require and in what timeframe?			
7	What elements are newsworthy?			

6 Stakeholder map