HERIOT WATT UNIVERSITY

Information Security Incident Management Procedures

September 2013

PROCEDURES

HERIOT-WATT UNIVERSITY
PROCEDURES
TO SUPPORT INFORMATION SECURITY INCIDENT MANAGEMENT POLICY
CONTENTS

Section **Page**

PROCEDURES

1. INTRODUCTION

These procedures underpin and should be read in conjunction with the Heriot-Watt University **Information Security Incident Management Policy**.

If you need to report an incident, please read sections two, seven and Appendix 1

If you receive an information security incident report or need to respond to an incident, please read from section three onwards.

2. HOW TO REPORT AN INFORMATION SECURITY INCIDENT

Please report any actual, suspected or potential breach of information security promptly as follows:

In office hours (UK time 9 a.m. – 5 p.m. Monday –Friday)

Breaches of IT or Information Security:

Contact the IT Help desk by one of the following methods

- Telephone +44 (0) 131 451 4045
- Telephone from University phones on the Edinburgh campus: extension 4045
- Email: IThelp@hw.ac.uk

Breaches of physical security, stolen, lost and found IT and communications equipment and portable devices

Contact the Duty Security Supervisor in the Security Control Room at the Edinburgh campus by one of the following methods:

- Telephone +44 (0) 131 451 3500
- Telephone from University phones on the Edinburgh campus: Extensions 3500 or 2222(emergency number)
- Use red telephones in the shared/public areas at the Edinburgh campus to connect directly to Security Control Room

Out of hours: ALL information security incidents

Contact the Duty Security Supervisor in the Security Control Room at the Edinburgh campus.

Where possible use the incident reporting form (Appendix 1). This will enable the relevant details of the incident to be recorded consistently and communicated on a need to know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

3 HOW TO MANAGE THE RESPONSE TO AN INFORMATION SECURITY INCIDENT

3.1 Who needs to be involved?

On receiving the incident report, the senior officer on duty in the section receiving the report will contact the relevant Head of School, Institute or Service and one or more of the following Lead Officers as appropriate.

Use the **Information Security Incident response flowchart in** Appendix 4 as a guide.

If a report is received out outside office hours, the senior officer on duty should follow **the Information Security Incident escalation process in** Appendix 3.

Lead Officer for Breaches of IT security: Director of Information Services or designate (or School Computing Officer), liaising with Head of School, Institute or Service affected or their designate

Examples:

- Virus or other security attack on IT equipment, systems or networks
- Breach of IT and Communications Facilities Acceptable Use Policy

If the investigation of the incident requires access to a user's IT account e.g.in a case of suspected downloading of illegal material, this must be escalated to the Secretary of the University for approval.

Lead Officer for breaches of information security: Information Security Officer (Head of Heritage and Information Governance) liaising with Head School, Institute or Service affected or their designate and the Head of Risk and Audit Management

Examples: loss or unauthorised disclosure of

- medium or high risk confidential information
- personal data
- information and records of operational, legal or evidential value to the University

Lead Officer for breaches of physical security: loss or theft of devices or equipment: Security and Operations Manager or designate liaising with Head of School, Institute or Service affected or their designate Security and Operations Manager will, where appropriate, inform the police

Examples:

- lost or stolen laptop,
- attempted break in to secure server or records store

3.2 Assessing the risks and actions to be taken

The Lead Officer should use the guidance in section 2.2 and 2.3 of the Incident Management Checklist in Appendix 2 and the Information Security Incident escalation process in Appendix 3 to decide whether the incident is of

Low Criticality (GREEN) which can managed within normal operating procedures

Medium Criticality (AMBER): a serious adverse incident, requiring assistance from designated Officers or specialist support teams outside the business unit. Most incidents will fall into this category.

High Criticality (RED) a major incident requiring significant University resource beyond normal operating procedures, requiring escalation to the Major Incident Plan

This will help determine:

- Who should take the lead in containment and recovery from the incident
- Who should take the lead in investigating the incident
- Who else needs to assist
- What resources they need
- What can be done to recover any losses
- What can be done to limit the damage caused by the incident
- Whether the incident needs to be reported to the police

The lead officer will inform the other responsible officers, listed below, and liaise with them and the relevant members of their teams as appropriate to resolve the incident.

- Director of Information Services
- Information Security Officer
- Security and Operations Manager
- Head of Risk and Audit Management

The Lead Officer will liaise with the other responsible officers and information/systems owners to consider the risk factors in section 2.3 of the incident management checklist and take the actions necessary to manage the incident and mitigate its impact.

3.3 Who else needs to be informed?

The **Information Security Officer** will liaise with the other Responsible Officers and the Director of Governance and Legal Services to determine whether it is necessary to notify the breach to others beyond the reporting chain of command within the University.

If the incident is a breach of **physical security**, such as the theft of a laptop, the Security and Operations Manager or designate will call the police promptly as part of the standard operating procedure.

PROCEDURES

If an incident involves other alleged criminal acts such as suspected downloading of illegal material, the Secretary of the University or designate will ask the police to investigate.

If the breach involves the loss of a University mobile phone or tablet the Security and Operations Manager or designate will inform Procurement Services who will notify the service provider and arrange for a replacement.

If the breach involves the loss or disclosure of personal data:
The Information Security Officer and Director of Governance and Legal Services will consider whether it is necessary to

Inform the individuals concerned
E.g. If individuals need to act on this information to mitigate risks, for example by cancelling a credit card or changing a password

Notify the UK Information Commissioner of the breach
E.g. if

- a large volume of personal data has been lost and there is a real risk of individuals suffering some harm e.g. an unencrypted laptop containing the names, addresses, dates of birth and national insurance numbers of 1000 staff
- personal data of a small number of individuals if there is significant risk of the individuals suffering substantial harm e.g. paper financial records of 50 individuals; an unencrypted memory stick containing highly sensitive personal data about one vulnerable individual

If the breach involves the loss or disclosure of other medium or high risk confidential information such as research data received or processed under conditions of confidentiality it may be necessary to notify the supplier of the information and other external stakeholders e.g. a regulatory body, grant funder

In each case the notification should include as a minimum

- a description of how and when the breach occurred
- what information was involved
- what action has been taken to respond to the risks posed by the breach

The Information Security Officer and the Director of Governance and Legal Services will identify any significant risks that need to be escalated as a matter of urgency to the Risk Management Strategy Group and addressed though the University's Risk Management Plan and Disaster Recovery Plan.

3.4 Reviewing the incident

The Responsible Officers will meet to review the incident, ensure that all appropriate actions have been taken to mitigate its impact and identify further action needed to reduce the risk of a future breach of this kind.

The Lead Officer will use the incident checklist and reporting tool to produce an incident report setting out:

- A summary of the incident
- How and why the incident occurred
- Actions taken to resolve the incident and manage its impact
- Impact of the incident (Operational, financial, legal, liability, reputational)
- Risks of other adverse consequences of the incident (Operational, financial, legal, liability, reputational)
- Any further remedial actions required to mitigate the impact of the breach
- Actions recommended to prevent a repetition of the security breach
- Resource implications or adverse impacts, if any, of these actions

4. MONITORING AND MANAGING RISKS

The Information Security Officer will receive reports of all information security incidents and use these to compile a central record of incidents. The Information Security Officer will report on these to the Information Security Group and thence to the Secretary of the University at least on a quarterly basis in order to identify lessons to be learned, patterns of incidents and evidence of weakness and exposures that need to be addressed.

For each **serious** or **major** incident the Information Security Group will lead a review to consider and report to the Secretary of the University

- What action needs to be taken to reduce the risk of future breaches and minimise their impact?
- Whether policies procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach?
- Are there weak points in security controls that need to be strengthened?
- Are staff and users of services aware of their responsibilities for information security and adequately trained?
- Is additional investment required to reduce exposure and if so what are the resource implications?

The Information Security Officer will liaise with the relevant Head of School, Institute or Service and the Head of Risk and Audit management to update the local or corporate risk register/s.

5. RELATED POLICIES AND PROCEDURES AND FURTHER REFERENCE

These procedures form part of the University Information Security Policy Framework and its underpinning policies, procedures and guidance which are published on the University website at:
http://www.hw.ac.uk/archive/ism-policies.htm

6. FURTHER HELP AND ADVICE

For further information and advice about these procedures and any aspect of information security, contact

Ann Jones
Head of Heritage and Information Governance ,
0131 451 3219
Email a.e.jones@hw.ac.uk
or foi@hw.ac.uk

7. DEFINITIONS

Information

The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media.

Confidential information

The definition of confidential information can be summarised as:

- Any personal information that would cause damage or distress to individuals if disclosed without their consent.

- Any other Information that would prejudice the University's or another party's interests if it were disclosed without authorisation.

A more detailed definition can be found in the Policy for secure use of confidential information on portable media

Information security incident

Any event that has the potential to affect the confidentiality, integrity or availability of University information in any format. Examples of information security incidents can include but are not limited to:

- The disclosure of confidential information to unauthorised individuals
- Loss or theft of paper records, data or equipment e.g. laptops, smartphones or memory sticks, on which data is stored

- Inappropriate access controls allowing unauthorised use of information
- Suspected breach of the University IT and Communications Acceptable Use Policy
- Attempts to gain unauthorised access to computer systems, e, g hacking
- Records altered or deleted without authorisation by the data "owner"
- Virus or other security attack on IT equipment systems or networks
- "Blagging" offence where information is obtained by deception
- Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information left unlocked in accessible area
- Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information.
- Covert or unauthorised recording of meetings and presentations
- Insecure disposal of paper documents or IT and communications equipment allowing others to recover and read confidential information

Information Security Management System

"That part of the overall management system based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organisational structure, polices, planning activities, responsibilities, practices, procedures, processes and resources."
BS ISO/IEC 27001: 2005: Information Security

8. PROCEDURE VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V3	V2 13.08.2012	REALISM Project Board	Minor updates for clarity and consistency

APPENDIX 1: INFORMATION SECURITY INCIDENT REPORT

To be completed by the person reporting incident or the member of staff who receives a verbal report by telephone.

Confidentiality notice
Information about actual and suspected information security incidents is confidential and must be shared only with staff with designated responsibilities for managing such incidents. Personal data must be shared on a need to know basis: only those staff who need this information to deal with the incident and its consequences should know the identity of individual/s involved.

1 Incident report	
Date of incident	**Place of incident**
Name of person reporting incident	
Contact details: email; telephone/address	
Brief description of incident or details of the information lost	
Brief description of any action taken at the time of discovery	
For University use	
Incident reference number	
Received by	**On**
Forwarded for action to	**On**

APPENDIX 2 – INFORMATION SECURITY INCIDENT MANAGEMENT CHECKLIST AND REPORTING TOOL

Type of incident	**Lead Officer**
Breaches of IT security	Director of Information Services or designate (or School Computing Officer),
Breaches of information security	Information Security Officer (Head of Heritage and Information Governance)
Breaches of physical security, loss or theft of devices or equipment:	Security and Operations Manager or designate

2.1: Incident summary: to be completed by Lead Officer	
Name of Lead Officer	Role
Incident reference number	
Summary of the actual or suspected security breach	
Date of incident	
School/s Institutes/Professional Services affected	
People involved in/affected by the incident, (such as staff members, students, contractors, external clients) **Personal data must be shared on a need to know basis: only those staff who need this information to deal with the incident should know the identity of the individual/s concerned.**	

Section 2.2: Managing the incident: who needs to be involved	
Please use this checklist below to assess the severity of the incident and determine whether it should be managed as a HIGH, MEDIUM or LOW Critical Incident.	
High Criticality (RED) Is this a major incident?	**YES/NO**
Does containment and recovery, OR the consequences of the loss OR unavailability of the asset Require significant University resource to manage beyond normal operating procedures?	**IF YES:** Inform the Secretary of the University and follow the Major Incident Plan.
IF NO:	
Medium Criticality (AMBER): Is this a serious adverse incident?	**YES/NO**
Do containment and recovery require assistance from designated Officers or specialist support teams outside the business unit? OR Does the breach require a notification to the University's senior managers?	**IF YES:** The Lead Officer will inform the other responsible officers and decide who else needs to assist or be made aware of the breach. **Responsible officers** ▪ Director of Information Services or designate ▪ Information Security Officer ▪ Security and Operations Manager ▪ Head of Risk and Audit Management ▪ Head of School, Institute or Service affected by the incident **Others who may need to be involved or assist** ▪ Director of Governance and Legal Services ▪ Academic Registrar and Deputy Secretary ▪ Director of Human Resources ▪ Director of External Relations
IF NO	
Low Criticality (GREEN)	**YES/NO**
Can the consequences of the security breach, loss or unavailability of the asset can be managed within normal operating procedures?	**If YES** • Manage incident with the Head of the relevant School, Institute or Service • Send a report of the incident and investigation to the Information Security Officer, who will keep a central record of all such incidents and copy to the following **Responsible officers**: ▪ Director of Information Services ▪ Security and Operations Manager ▪ Head of Risk and Audit Management ▪ Head of School, Institute or Service affected by the incident

PROCEDURES

2.3 Assessing the risks and actions to be taken	
The Lead Officer should liaise with the other responsible officers and information/systems owners to consider the following risk factors when assessing, managing and investigating the incident. This list is not intended to be prescriptive and other relevant factors and issues should be recorded as necessary	
Does the incident need to be reported immediately to the police?	**YES/NO**
Risk Factor	**Details and action required**
Which IT systems, equipment or devices are involved in the security breach?	
What information has been lost or compromised?	
How much information has been lost?	
Is the information unique?	
If the incident involves the loss of a laptop or portable device how recently was the information it held backed up onto central IT systems?	
How important is the information or system to the business process or function? Does it include records of operational, legal or evidential value to the University?	
Is it business-critical? Do users rely on access to this particular information asset or can they use reliable electronic copies or alternative manual processes e.g. paper files if the information asset is unavailable?	
How urgently would access need to be restored to an information asset to resume business or, if a workaround will keep business moving in the short term, to return to the required standard of service?	
Will the loss or compromise of the information have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	

PROCEDURES

Is the information bound by any contractual security arrangements e.g. to research sponsors?	
Is any of the information confidential? Please provide details of any types of information that fall into any of the following categories.	
HIGH RISK personal data	
Sensitive personal information (as defined in Section 2 of the Data Protection Act 1998 relating to an identifiable individual's 1. racial or ethnic origin; 2. political opinions; 3. religious or other beliefs; 4. membership of a trade union; 5. physical or mental health or condition; 6. sexual life; 7. proven or alleged offences, including any legal proceedings and their outcome e.g. a court sentence imposed on the individual	
Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as national insurance numbers and copies of passports and visas	
Personal information relating to vulnerable adults and children	
Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed	
Spread sheets of marks or grades obtained by students, information about individual cases of student discipline	
Sensitive negotiations which could adversely affect individuals.	
Security information that would compromise the safety of individuals if disclosed.	

Any other personal information that would cause damage or distress to individuals if disclosed without their consent	
Other categories of "high risk" information	
Unpublished research data that has been received or created under conditions of confidentiality and would if lost or disclosed significantly impact on the success of a research project, research income. REF outputs or knowledge transfer	
Information received in confidence .e.g. legal advice from solicitors, trade secrets and other proprietary information received from contractors, suppliers and partners	
Information that would substantially prejudice the University or another party's intellectual property rights, commercial interests or competitive edge if it were disclosed	
Information relating to high profile/high impact strategy or policy development before the outcomes have been decided and announced.	
Information that would compromise the security of buildings, equipment or assets if disclosed.	

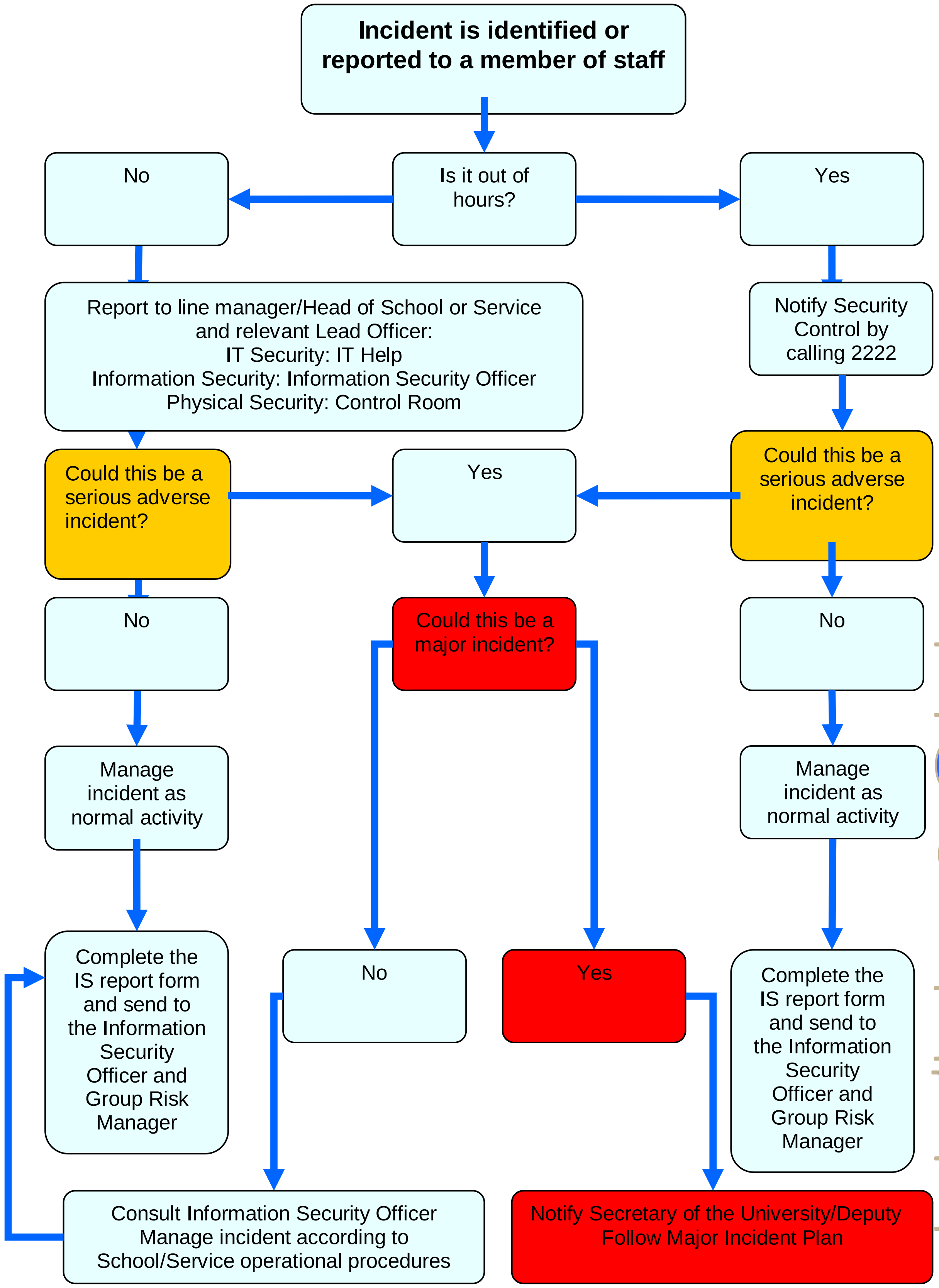
2.4 Who else needs to be informed	
Reported to Police?	YES/NO If YES notified on Incident ref:
Reported to Information Security Officer (if not the Lead Officer)	Date
Reported to other internal stakeholders	Details, date
Major risks escalated to Risk Management Strategy Group	YES/NO If YES: Date
For Information Security Officer use:	
Notification to Information Commissioner's Office	YES/NO If YES notified on [date]
Notification to data subjects	YES/NO If YES notified on [date]
Notification to other external, regulator/stakeholders	YES/NO If YES notified on

PROCEDURES

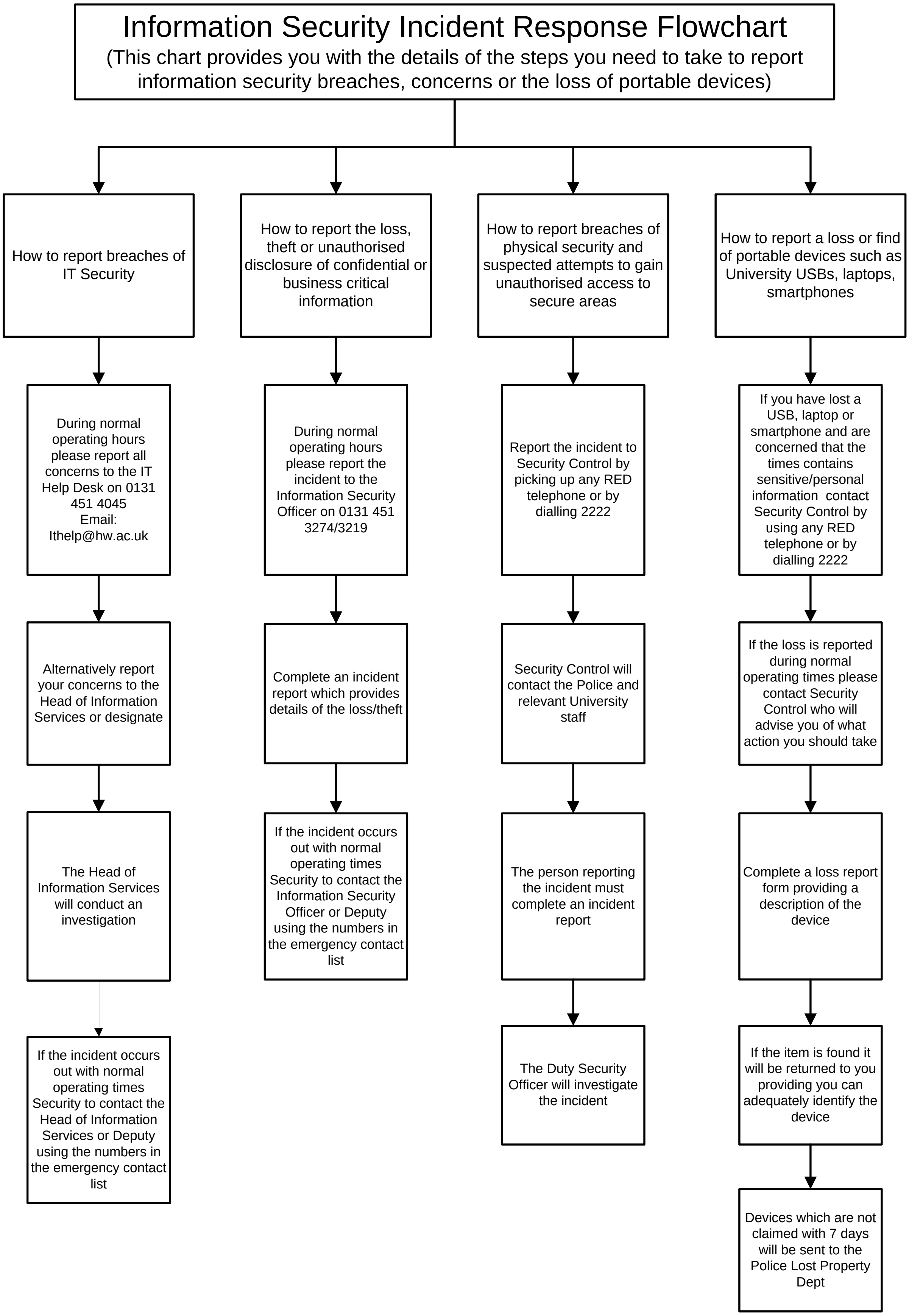
2.5 Reviewing the incident
The Responsible Officers should meet to review the incident, ensure that all appropriate actions have been taken to mitigate its impact of the incident and to identify further action needed to reduce the risk of a future breach of this kind
How and why the incident occurred
Actions taken to resolve the incident and manage its impact
Impact of the incident (Operational, financial, legal, liability, reputational)
Risks of other adverse consequences of the incident (Operational, financial, legal, liability, reputational)
Any further remedial actions required to mitigate the impact of the breach
Actions recommended to prevent a repetition of the security breach
Resource implications or adverse impacts, if any, of these actions

2.6 Monitoring and managing risks	
To be completed by Information Security Officer	
Recorded in incident register	Date
Major risks escalated to Risk Management Strategy Group	YES/NO If YES: Date
Risk register for the relevant School, Institute or Service updated	Date By (officer)
Incident report to Information Security Group	Date
Reviewed by Information Security Group on	Date
Recommendations by Information Security Group to reduce risk or minimise impact:	
Policies, procedures or reporting lines to be clarified or strengthened	
Improvements in security controls	
Training and awareness raising	
Other actions	
Additional investment- resource implications	
Reported to Secretary of the University /Risk Management Strategy Group on	[date]
Actions agreed on [date]	
Responsible Officers	
Timescale	

APPENDIX 3: INFORMATION SECURITY INCIDENT ESCALATION PROCESS


Incident is identified or reported to a member of staff
No
Is it out of hours?
Yes
Report to line manager/Head of School or Service and relevant Lead Officer:
IT Security: IT Help
Information Security: Information Security Officer
Physical Security: Control Room
Notify Security Control by calling 2222
Could this be a serious adverse incident?
Yes
Could this be a serious adverse incident?
No
Could this be a major incident?
No
Manage incident as normal activity
Manage incident as normal activity
Complete the IS report form and send to the Information Security Officer and Group Risk Manager
No
Yes
Complete the IS report form and send to the Information Security Officer and Group Risk Manager
Consult Information Security Officer
Manage incident according to School/Service operational procedures
Notify Secretary of the University/Deputy
Follow Major Incident Plan

APPENDIX 4: INFORMATION SECURITY INCIDENT RESPONSE FLOWCHART



Information Security Incident Response Flowchart

(This chart provides you with the details of the steps you need to take to report information security breaches, concerns or the loss of portable devices)

How to report breaches of IT Security

During normal operating hours please report all concerns to the IT Help Desk on 0131 451 4045 Email: Ithelp@hw.ac.uk

Alternatively report your concerns to the Head of Information Services or designate

The Head of Information Services will conduct an investigation

If the incident occurs out with normal operating times Security to contact the Head of Information Services or Deputy using the numbers in the emergency contact list

How to report the loss, theft or unauthorised disclosure of confidential or business critical information

During normal operating hours please report the incident to the Information Security Officer on 0131 451 3274/3219

Complete an incident report which provides details of the loss/theft

If the incident occurs out with normal operating times Security to contact the Information Security Officer or Deputy using the numbers in the emergency contact list

How to report breaches of physical security and suspected attempts to gain unauthorised access to secure areas

Report the incident to Security Control by picking up any RED telephone or by dialling 2222

Security Control will contact the Police and relevant University staff

The person reporting the incident must complete an incident report

The Duty Security Officer will investigate the incident

How to report a loss or find of portable devices such as University USBs, laptops, smartphones

If you have lost a USB, laptop or smartphone and are concerned that the times contains sensitive/personal information contact Security Control by using any RED telephone or by dialling 2222

If the loss is reported during normal operating times please contact Security Control who will advise you of what action you should take

Complete a loss report form providing a description of the device

If the item is found it will be returned to you providing you can adequately identify the device

Devices which are not claimed with 7 days will be sent to the Police Lost Property Dept