Resources for Chapter 11 – When things go wrong: non-conformities and incidents

RESOURCES

- Developing an Information Security Incident Response Plan based on ISO/IEC 27035:2011 – University of Oxford
- Example of an information security incident response scheme
- Information Security Service: Information Security Incident Management Process – UCL
- Investigations and Data Access Policies – University of York, case study
- Data breach – case study

Developing an Information Security Incident Response Plan based on ISO/IEC 27035:2011 – University of Oxford

Introduction

Information security incidents are, one way or another, inevitable but the response to an incident can still reduce the overall risk to an organisation by way of reducing the impact of any given incident. The key to good incident management is good communication and ensuring all stakeholders are aware of their roles and responsibilities. In order to achieve this, roles, responsibilities procedures and protocols need to be defined, agreed and tested. ISO/IEC 27035:2011 Information Technology – Security techniques – Information security incident management provides the outline of one method for implementing an incident response scheme and this study documents some of the applications and lessons learned from following such an approach in a University setting.

Motivation for Developing an Incident Response Plan

Having a formal incident response plan can help to ensure that an organisation is well informed of the current threat landscape and risks. This can be particularly important in devolved environments such as Universities where individual units may handle incident response well in isolation. Where there is no overall coordination, formal escalation or reporting of security incidents it is unlikely that lessons learned will be followed up and acted upon or shared with other relevant parts of the organisation. Similarly if incidents are escalated to senior members of an organisation it is important that those senior stakeholders understand the information they are being presented with, why they are being informed and what action they need to take. The goals of an incident response plan are therefore to ensure that:

- Incidents are detected and reported in a timely manner
- Incidents are properly investigated and handled efficiently and effectively
- The impact of incidents is minimized and action taken to prevent further damage
- Incidents are communicated appropriately and appropriate levels of University management are involved in the response
- External bodies or data subjects are informed as required
- Evidence is gathered, recorded and maintained appropriately
- Details of incidents are recorded and documented
- Incidents are reviewed and subsequent improvements made to policies and procedures

Observations and lessons learned

Policy and Governance It is critical to the success of an incident response plan to be ratified and signed off at a senior level within the organisation. Typically this will be a senior information security board or other senior committee that owns information security risk. An incident response policy should first be agreed so that it is clear what the intentions of the plan are and in order that progress (and problems) can be monitored and measured. Although the policy and plan will be owned by a senior board it should be made accessible and communicated to all departments within the organisation.

Incident Detection/Reporting

Clear guidance needs to be given on when to report incidents, what to report, how and to whom. Many incidents may not be reported centrally either because they are not recognised as security incidents or because policy and/or process for reporting has not been widely communicated and understood. As a result the number and type of incidents dealt with across an organisation will not tell the whole story, hampering informed decision making based on a true understanding of risk.

The definition of a security incident may need to be reviewed. Typically IT security related incidents have been dealt with in isolation but, with a general move towards greater focus and maturity in information security, it is now necessary to expand the definition of an incident to include breaches of information security regardless of the format. It is, however, important to clearly define when events become incidents and should be reported. To this end guidance should be produced for individual departments to understand clearly what types of incident need to be reported and how. For example ongoing incidents may need to be reported immediately as assistance or escalation is required (e.g. compromised server, stolen laptop with personal data). Other incidents might only be useful for statistical purposes and they can be reported periodically (e.g. number of malware infections dealt with by a department in the past month).

Whether an incident should be reported immediately will depend on the potential impact on the organisation as a whole. Therefore criteria should be agreed in advance with senior stakeholders and appropriate guidance should be provided to local departments. Incidents should be reported within departments or sections initially and the guidance should be used to make a decision as to whether to report centrally. A single point of contact should be provided for reporting centrally and, ideally, will be made use of by specific departmental liaisons. However it should be recognised that incidents will be reported to alternative contacts. It is therefore important to ensure that staff within departments (particularly those providing central services) are aware of where to forward incident reports.

Communication, Coordination and Escalation

Incidents should be communicated and handled efficiently. This requires all stakeholders in incident response to be identified, informed in a timely manner and be aware of their responsibilities. Where an incident will (or may) have an adverse impact on an organisation's primary assets then senior members of the organisation should be made aware, as soon as is practicable, in such a way as to make it clear what the impact of an incident is (or might be) and what is required of them. This may be simply for information purposes (e.g. to warn of potential impact) or to require some intervention, backing or ruling on reactive measures. Particularly in a devolved environment, tensions often arise between incident handlers and service providers. The owner of a website used (for example) for receiving job applications will be particularly keen to get the site up and running again quickly, whilst the incident handler will not be happy to restore the site until the vulnerability has been identified and fixed. Where such tensions arise it is extremely useful to have the backing of senior stakeholders within the organisation and/or allow senior stakeholders to make informed decisions on corrective actions based on the risk vs. the impact to the business.

A clear and concise format for escalation reports should be agreed upon in advance. Escalation reports might (for example) include the current impact, potential impact and how likely that is, as well as any specific action required of anyone receiving the reports. This will lead to far fewer queries when escalating incidents thus considerably improve efficiency and speed of communication.

Responding to incidents often requires coordination amongst different business functions. Depending on the nature of the incident this could include physical security services, legal services, data protection offices, the press office etc. Having a small core of initial incident responders and senior stakeholders will mean that the right people are immediately informed of incidents and may bring other stakeholders in (such as legal services and the press office) as required. Ensuring the incident response and escalation team include senior stakeholders representative of the organisation will help to ensure that appropriate backing is received when dealing with incidents. To ensure that stakeholders are fully aware of mitigating actions that are taken regular updates (particularly changes in status) should therefore be communicated to the immediate response team.

Classifying and Categorisation

In order to ensure that senior stakeholders get the information they require and, are appropriately informed about incidents, it is important to ensure those stakeholders agree in advance the circumstances under which they should be informed. Generally this means categorising incidents in terms of their nature and impact and so impact criteria should be defined and agreed. So as not to create overly complex and new impact criteria it is useful to use existing criteria where possible – for example using criteria for risk assessment. The number of overall incident classifications (e.g. Major, Moderate, Minor) should also be kept to a minimum (similarly to information classification schemes).

It is also worth noting that the criteria used for escalation of incidents is primarily used as a tool by initial incident responders but is aimed at senior stakeholders. In other words incident responders tend to be experienced and know when something should be escalated. The impact criteria can therefore be seen as a means for initial incident responders to explain why an incident has been escalated. If the criteria are not useful for incident responders in this way they should be revised.

Roles and responsibilities

All members of the incident handling team should understand their roles and responsibilities, which should include providing appropriate support and leadership in dealing with incidents. Having these agreed in advance is, again, advantageous though specific roles and actions may need to be assigned throughout the incident lifecycle. For example, incidents should have a designated incident owner who is responsible for making executive decisions and providing senior support for a given incident. This person should be authorised and readily available throughout the duration of the incident so as to avoid unnecessary delays in resolving incidents.

It is particularly beneficial to understand and agree the responsibilities of initial incident handlers, particularly in terms of ascertaining the right level of information in order to make an informed decision as to the potential impact of an incident and maximise efficiency when incidents are escalated. For example, agreeing in advance with the data protection officer the questions that need to be asked in terms of the level of personal data involved in a breach means that the initial incident handler can complete the triage stage. This allows stakeholders, such as the data protection officer, to make quicker, informed decisions and reduces the amount of correspondence and communication channels required. Incidents involving personal data (or potentially involving personal data) are now dealt with much more efficiently.

Summary of main lessons learned

- Having an incident response plan improves the efficiency of handling major incidents and leads to a more coordinated, university-wide approach.
- Policies for incident response should be agreed in advance and signed off by senior management as should subsequent processes in the scheme
- The plan should be simple to follow.
- Criteria for escalation and reporting should be agreed with senior stakeholders in advance.
- Roles and responsibilities of stakeholders should be agreed in advance.
- Good communication of incidents means that senior stakeholders are informed quickly and understand the impact of security incidents
- Specific incident owners should be explicitly assigned for each incident
- An appropriate governance structure is required in order to present reports on incidents, findings, vulnerabilities and risks
- All university members should understand what they should report and how they should report it.

Example of an information security incident response scheme

Introduction

The purpose of this scheme is to provide detailed documentation describing the policies activities and procedures for dealing with information security events and incidents. The scheme includes definitions of information security events and incidents and should be used as a guide for:

- responding to information security events
- determining whether an event becomes an incident
- detecting and reporting information security events/incidents
- classifying information security incidents
- response to, and escalation of, information security incidents
- roles and responsibilities for dealing with information security incidents
- identifying lessons learnt and making improvements

Information Security Incident Management Policy

Scope

This policy forms part of the information security management framework and supplements the University's information security policy. It applies to events and incidents affecting any University information assets or information system. It applies to and will be communicated to all those with access to University information systems, including staff, students, visitors and contractors.

Objective

The University recognizes the importance of, and is committed to, effective information security incident management in order to help protect the confidentiality and integrity of its information assets, availability of its information systems and services, safeguard the reputation of the University and fulfil its legal and regulatory obligations.

The University will ensure that:

- Incidents are detected and reported in a timely manner
- Incidents are properly investigated and handled efficiently and effectively
- Incidents are communicated appropriately and appropriate levels of University management are involved in the response
- The impact of incidents is minimized and action taken to prevent further damage
- Incidents are reviewed and subsequent improvements made to policies and procedures
- Evidence is gathered, recorded and maintained appropriately
- Incidents are recorded and documented
- External bodies or data subjects are informed as required

Policy

1. Information systems which are known to be (or suspected of being) compromised will be isolated from the University network until the incident has been investigated, resolved and risks sufficiently reduced.
2. Guidance and procedures for the detection, assessment, communication, reporting and escalation of security vulnerabilities, events and incidents will be provided via the information security website, training programs and other communication channels.
3. All information security incidents must be reported via the appropriate management channels.
4. Responsibilities for the reporting and escalation of security vulnerabilities, events and incidents should be clearly defined and communicated to all relevant personnel.
5. Security events and incidents should be assessed according to the event/incident classification scale provided via the information security toolkit and, where necessary, escalated accordingly.
6. An information security incident response team (or teams) comprising representatives from all relevant parts of the University, shall coordinate the management of and response to incidents which require escalation in accordance with an Information Security Incident Response Plan.
7. Incidents involving personal data will be reported to the Data Protection Officer.
8. Incidents which involve personal safety, security or require the involvement of law enforcement will be reported to the head of physical security.

9. Details of the Information Security Incident Response Plan will be made available via the information security website.

10. All information security incidents will be recorded for later analysis.

11. Post incident reviews will be carried out in order to identify where improvements in policies, procedures and information security controls can be made.

12. The types, volumes and impact of security incidents will be recorded and reviewed and summary reports will be used as input to the University's information security risk register.

13. Specific incident reports will be reviewed by the Information Security Working Group who may advise on corrective action in the future.

14. Information security incident procedures will be communicated to all relevant personnel and tested periodically.

15. Technical support and guidance will be provided by the IT department.

Information Security Incident Response Team (ISIRT)

The ISIRT refers to the group of people who will be the first responders for information security incidents and will act as the point of contact for information security incidents. The ISIRT will be responsible for the initial response, mitigation and (where appropriate) escalation of information security incidents. The roles and responsibilities for the ISIRT are as follows:

Computer Security and Incident Response Team (CSIRT)

The CSIRT are responsible for:

- Monitoring network traffic to identify compromised or potentially compromised systems within the University network;
- Receiving internal and external reports on compromised systems;
- Protecting the security and integrity of the University backbone network and its core ;information systems and services by blocking network access to any compromised machine;
- Informing and liaising with local IT staff to ensure that computer security incidents are dealt with promptly and effectively;
- Ensuring that compromised systems are fully cleaned and patched against known vulnerabilities, or the risk otherwise mitigated, before being reconnected to the network;
- For providing advice and guidance on dealing with computer and network security;
- Maintaining a register of computer security incidents;
- Initial investigation into the type and quantity of personal (or otherwise confidential) data involved in a compromise;
- Appropriate escalation of computer security incidents in accordance with the information security incident management scheme/plan.

Information Security Officer

The Information Security Officer is responsible for:

- Coordination of the ISIRT with regards incident response
- The maintenance and communication of the incident response policy and scheme;
- Creating, maintaining and communicating the information security incident response scheme, incident classification scale and other relevant procedures and guidance;
- Coordination of University-wide responses to information security incidents via the crisis/escalation team;
- Receiving reports on information security incidents and breaches of the information security policy;
- Appropriate escalation of information security incidents in accordance with the information security incident management scheme/plan;
- Reporting incidents involving personal data to the Data Protection Officer.
- Reporting of incidents to other appropriate bodies in a timely manner;
- Maintaining and updating the information security risk register to reflect recorded incidents;
- Writing and presenting appropriate incident reports to the Information Security Working Group and information systems/risk owners and including recommended remediations and lessons learnt.

Crisis/Escalation Team

Some incidents will require escalation above the ISIRT in order that senior management within the University are made aware of, and may respond accordingly, to serious and potentially serious information security incidents. The Crisis/Escalation Team consists of senior members of relevant University departments. Not all members of the Crisis/Escalation Team will need to be alerted to all information security incidents immediately. The classification scheme and requirements for escalation set out below will be used by the ISIRT to determine when the various parts of the Crisis/Escalation Team will be called into action.

The Crisis/Escalation Team will be made up of a core set of senior staff and will therefore consist of (e.g.):

- Director of IT Risk Management
- Data Protection Officer
- Head of Compliance
- CIO
- The head of physical security

Additionally other key stakeholders will need to be informed, consulted and respond as appropriate. It will be the responsibility of the core Crisis/Escalation Team to report to relevant stakeholders and increase the crisis team appropriately. These stakeholders include but are not limited to:

- Press Office
- The Registrar
- HR
- Legal Services Office

Roles and Responsibilities for the Crisis/Escalation Team

The roles and responsibilities for the Crisis/Escalation Team are as follows:

Director of IT Risk Management

The Director of IT Risk Management is specifically responsible for:

- Authorizing corrective actions to be taken by the ISIRT.
- Overseeing, measuring and monitoring the performance of the ISIRT and incident response scheme.
- Providing senior support and seeking sufficient resource in order to successfully implement and maintain the incident response scheme
- Ensuring incidents are escalated appropriately to other members of the crisis/escalation team.
- Leading the coordination and response of the crisis/escalation team.

Data Protection Officer Responsibilities

The University's Data Protection Officer is responsible for:

- Receiving reports of known and potential data protection breaches
- Initiating and leading investigations into suspected or known data protection breaches
- Ensuring that information security breaches received directly are reported to the information security team
- Appropriate escalation of information security incidents in accordance with the information security incident management scheme/plan.
- Decisions to report and subsequent reporting of data protection incidents to the Information Commissioner
- Communication to relevant staff of correspondence with the Information Commissioner

Head of Compliance

- Receiving reports of incidents that have been escalated and confirming the classification of those incidents
- Ensuring that the Registrar, Press Office, Legal Services, HR and any other relevant senior stakeholders are fully informed and updated on the progression of incidents as appropriate
- Providing senior management support for the incident response scheme

CIO

- Receiving reports of incidents that have been escalated and confirming the classification of those incidents
- Advising on and authorizing mitigating actions and responses that either have a direct or indirect effect on the IT department, or that the IT department will implement but may have considerable implications for other departments and/or the University
- Providing senior management support for the ISIRT and the incident response scheme.

The Head of Physical Security

- Receiving reports of incidents that have been escalated
- Decisions to report information security incidents to law enforcement
- Reporting and liaising with law enforcement
- Responding to physical security issues as a result of information security incidents

Reporting and Escalation of Information Security Incidents

Information security events and incidents

For the purposes of the University's information security incident response scheme:

Information security events are described as:

Identified occurrences of systems, services or networks that have the potential to breach information security policies

Information security incidents are described as:

A single or series of unwanted events that compromise (or are likely to compromise) the confidentiality, integrity or availability of University data and/or breach University information security policies

Some examples of information security events and incidents can be found below:

Information security events	Information security incidents
Network scanning	Lost or stolen laptops or mobile devices
Brute force attempts/multiple login attempts	Server compromises
Unsuccessful SQL injection attacks	Botnet infections
	Successful SQL (or other code) injection attacks
	Compromised accounts (e.g. accounts spamming)
	Denial of Service attacks
	Unauthorised access to information systems

Reporting Security Incidents

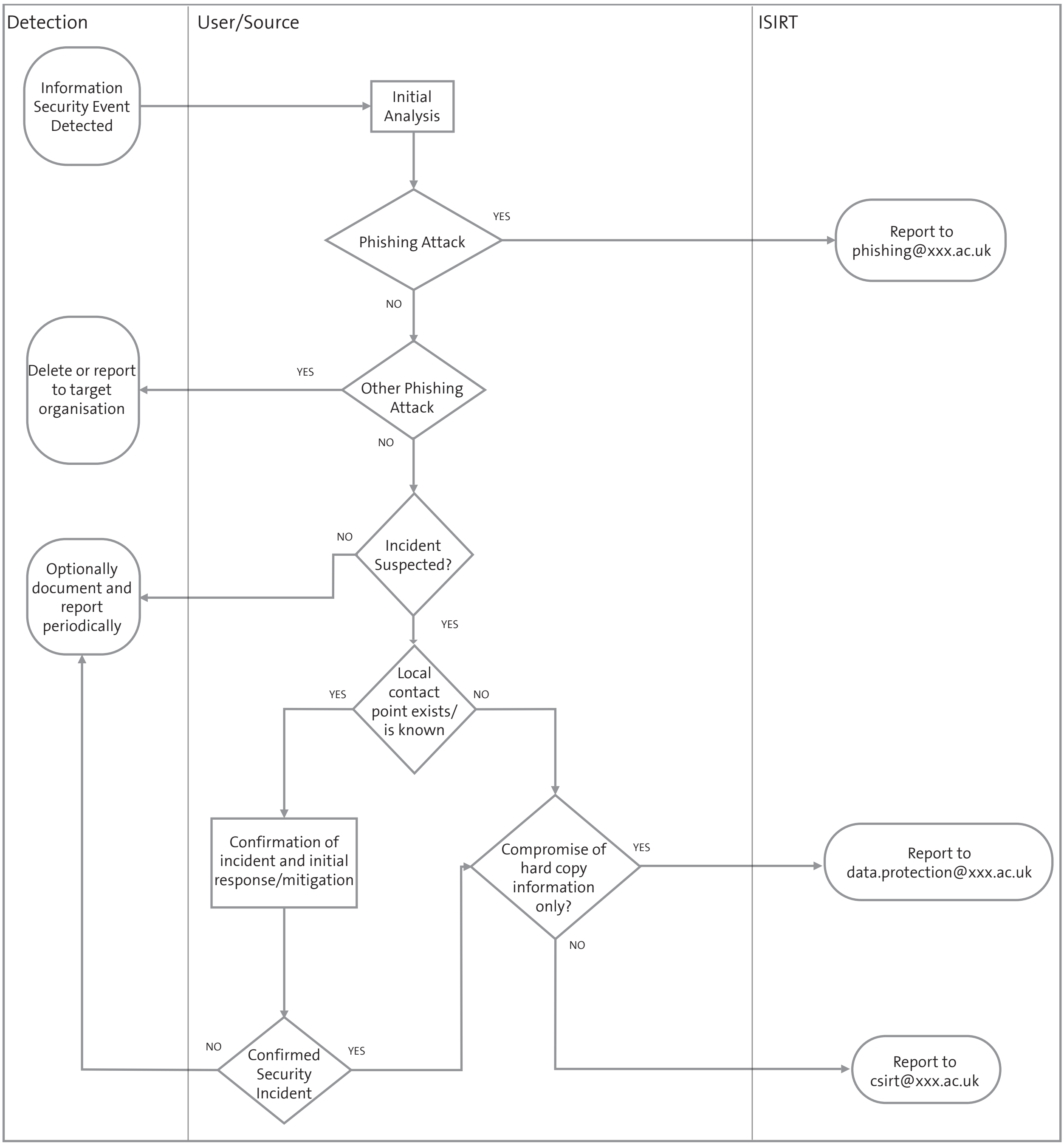
Reporting information security events and incidents can be important for information purposes (e.g. as an input into risk assessment) and/or in order to limit the impact of an incident. The purpose of this section is to provide information on what should be reported, when and to whom.

Information security **events** need not be reported immediately but **may** be reported periodically for information purposes. Usually information security events will be recorded automatically in log files relating to IT systems. These can be reported, by local IT support staff either manually or automatically. Other information security events should be reported to a local point of contact or via line managers who will decide whether to pass on the reports. No response should be expected to reports of information security events unless specific problems are identified.

All information security **incidents** must be reported. The University operates a devolved model for support when it comes to IT and information security, therefore users should usually report security incidents to identified local contacts. If there is any doubt then incidents should be reported to a user's direct line manager who will be responsible for deciding whether further action and/or reporting is required. Information security incidents should then be reported according to the initial incident reporting protocol described below.

Initial Incident Reporting Protocol

Information security incidents should be reported according to the following protocol:


Detection
User/Source
ISIRT
Information Security Event Detected
Initial Analysis
Phishing Attack
YES
Report to phishing@xxx.ac.uk
NO
Other Phishing Attack
YES
Delete or report to target organisation
NO
Incident Suspected?
NO
Optionally document and report periodically
YES
Local contact point exists/ is known
YES
NO
Confirmation of incident and initial response/mitigation
Compromise of hard copy information only?
YES
Report to data.protection@xxx.ac.uk
NO
Report to csirt@xxx.ac.uk
Confirmed Security Incident
NO
YES

Central Incident Response and Escalation

The ISIRT will be responsible for initial incident handling including investigation, initial response and classification of the incident in accordance with the classification scheme described in appendix A.

Initial incident handling will typically be handled by the CSIRT in accordance with their standard processes and practices. Additionally the CSIRT will make standard enquiries into the level of personal (or otherwise confidential) data that may have been exposed as a result of any incident. For the purposes of personal data details are given in Appendix B as to the information required by the Data Protection Officer.

The incident classification scheme will be used in the first instance for determining whether incidents should be escalated to other members of senior management throughout the University. Clearly the full impact of an incident will not be known at the time of initial response. The full impact will therefore be assessed in separate reporting and review of incidents at a later date. This information can be used assess how appropriate the escalation process was based on the classification at the time. Incidents will be escalated based on their current impact. In order that incidents are escalated appropriately therefore the classification scheme needs to take into account the potential impact. This is reflected by including "importance of information system" in the classification scheme. Incidents affecting important or critical information systems will therefore always create a higher level of alert.

In order to provide senior staff within the escalation team the information they require in order to determine what (if any) action is required, incidents escalation reports will include the following information:

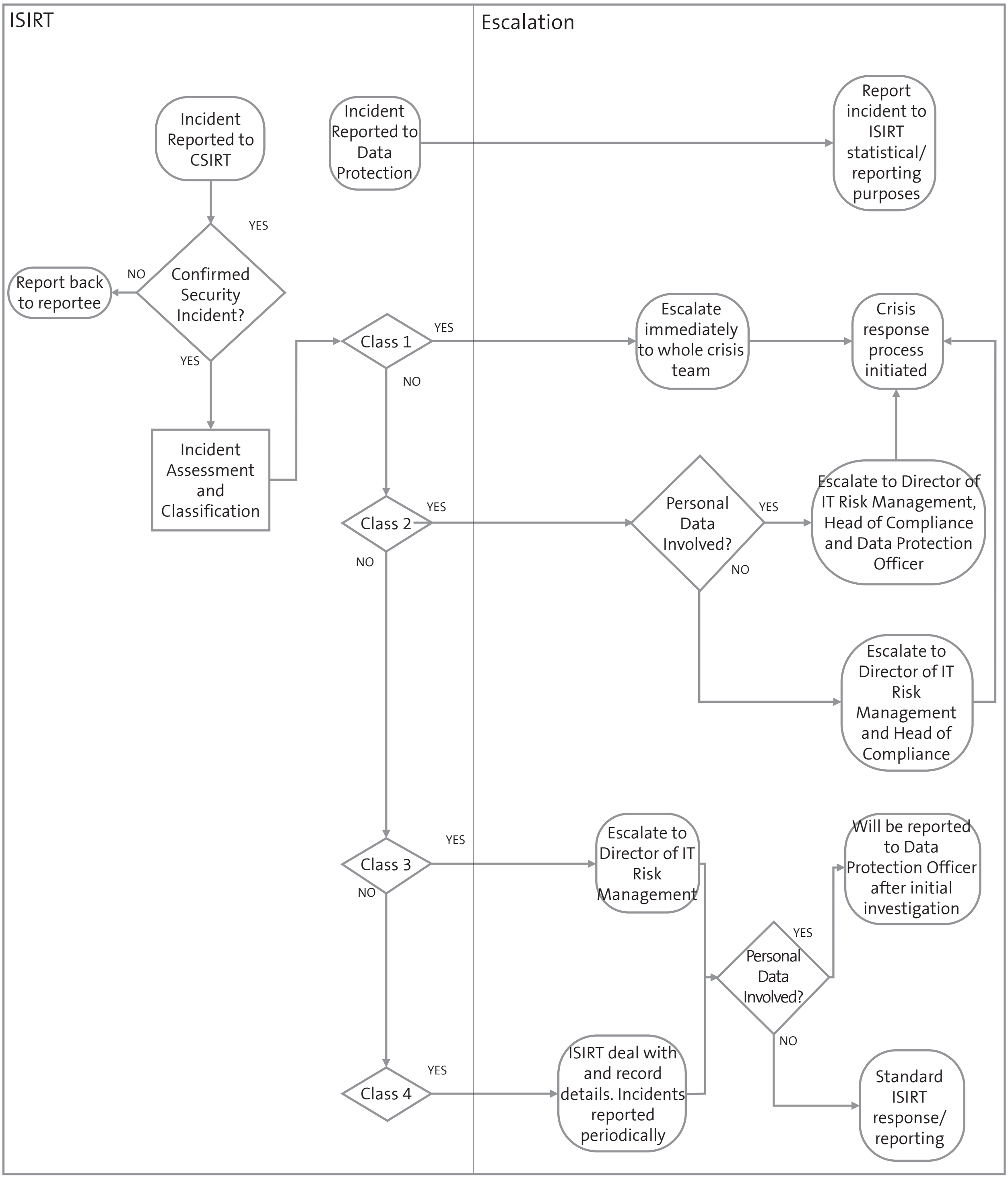
- Suspected date/time of incident
- Detection date/time
- Method of detection
- Incident category
- Current incident classification
- Basis for current classification
- Current status of investigation
- Current mitigating actions
- Potential incident classification
- Basis for potential incident classification (i.e. impact category)
- Estimate of actions/events that may lead to potential classification/impact
- Estimate of likelihood of potential classification/impact
- Notes and/or specific actions required of the Crisis/Escalation team

Updates to the status of an incident will be provided by the ISIRT either in accordance with the Crises/Escalation process described below or when the current classification of an incident changes (i.e. based on the current impact).

Further details on the process involved in escalating incidents according to the classification scheme can be found in Appendix C.

Incident Escalation Protocol

Incidents will be escalated by the ISIRT in accordance with the protocol described below:


ISIRT
Escalation
Incident Reported to CSIRT
Incident Reported to Data Protection
Report incident to ISIRT statistical/ reporting purposes
YES
NO
Report back to reportee
Confirmed Security Incident?
YES
Incident Assessment and Classification
Class 1
YES
NO
Escalate immediately to whole crisis team
Crisis response process initiated
Class 2
YES
NO
Personal Data Involved?
YES
NO
Escalate to Director of IT Risk Management, Head of Compliance and Data Protection Officer
Escalate to Director of IT Risk Management and Head of Compliance
Class 3
YES
NO
Escalate to Director of IT Risk Management
Will be reported to Data Protection Officer after initial investigation
Personal Data Involved?
YES
NO
Class 4
YES
ISIRT deal with and record details. Incidents reported periodically
Standard ISIRT response/ reporting

Crisis/Escalation Process

When information security incidents are escalated one person should take overall responsibility for coordinating the crisis response. It is assumed that this will be the Director of IT Risk Management unless explicitly stated for a particular incident. The lead coordinator will be responsible for ensuring the ISIRT provide updates as appropriate and will be responsible for overseeing and authorizing responsive action (including meetings of the response team), further escalation and eventually resolution of the incident. All members of the crisis response team have their responsibilities outlined above and are responsible for requesting relevant information for their area of responsibility.

Reporting of Information Security Incidents

All information security incidents will be reported at Information Security Working Group meetings and it is the responsibility of the Information Security Officer to ensure that incidents are presented and reported appropriately to this group. Class 3 and Class 4 incidents will be reported statistically to the IS Working Group noting any particular concerns or trends. Class 1 and Class 2 incidents will be reviewed in more detail noting the eventual impact and any lessons learned. Further details are presented in Appendix C.

Appendix A: Classification of Information Security Events/ Incidents

Incident Category

The following table provides categories and descriptions for various incident types:

Category	Description	Examples
Malware incident/ Malicious Code	Incidents primarily concerning malware infections or outbreaks.	Viruses, worms, Trojans, botnets, APTs, infostealer infections.
Technical Attack/ Unauthorised Access	Network attacks and attacks exploiting software vulnerabilities to execute code.	Network scanning, exploitation of vulnerability, backdoors, brute force attacks, SQL injection attacks, unauthorized elevation of privileges, buffer overflows, defacements, phishing
Denial of Service	Deliberate and accidental DoS attacks	DDoS and DoS attacks, electromagnetic radiation, jamming etc.
Technical Failure	Failures and faults in systems, infrastructure and services that support the running of information systems	Hardware failures, software failures, power failures, networking failures, air conditioning failures etc.
AUP Breach	Deliberate or accidental breaches of policies, regulations and/or laws	Unauthorised use of resources, copyright infringement, misconfiguration of devices, abuse of privileges, forging of rights
Physical compromise of information	Deliberate or accidental compromise of confidentiality, integrity, availability etc	Loss/theft of devices such as laptops, tablets, phones etc; Compromise of hard copy data such as Loss of documents (e.g. sent via post), theft of documents, transmission to wrong recipient (e.g. via fax).
Physical Damage	Deliberate or accidental physical events	Flood, wind, lightening, fire, theft loss, vandalism etc.
Other incidents	Catch all for not categorised	

Impact Categories

All incidents will be categorized according to their impact. The impact will be either CRITICAL, MAJOR, MODERATE or MINOR based on the impact categories below. The greatest impact from the five different types of impact will determine the impact category assigned to an incident. When incidents are reported the current and potential impact should be reported along with some indication of how likely escalation may be (or what would need to happen for the potential impact to be realized)

Importance of Information System

Category	Description	Examples
Critical	Business-critical systems fundamental to the daily operations of the University supporting teaching, learning, research or the administration of the University. Compromise of a critical system would cause significant disruption or reputational damage to the University. 'Significant' in this context is defined as impacting the operations of multiple University departments; the disruption may be more significant at certain times of the year.	Email systems; Financials systems; Core Infrastructure systems (such as routers, DNS); Primary University Web Server
Major	**EITHER** A system that is critical to the operations of a single department but may also impact other departments. Loss of a Major system would cause significant disruption to the affected department and may cause inconvenience to other departments. **OR** A system that supports multiple departments but is not business-critical. Loss of a Major system would cause inconvenience to multiple departments.	Departmental directory server; Main departmental webservers;
Moderate	A system that supports services internal to individual departments. Loss of a moderate service would cause inconvenience to the department in question.	Departmental web servers;
Minor	All other systems	Desktops; Laptops; Mobile devices

Service impact

Category	Description	Examples
Critical	University is no longer able to provide some core services to any users.	Central Email service is unavailable; Backbone network connectivity is lost or significantly impaired.
Major	**University is unable to provide a core service to a subset of users**	Central email relays blacklisted for certain emails
Moderate	University is able to provide core services to users but secondary services may be unavailable and/or services may be impaired for a period of time.	
Minor	No effect on the University's ability to provide core services to users.	

Privacy Impact

Category	Description	Examples
Critical	**EITHER** A potential or known breach of confidentiality where the release of data could cause a significant risk of individuals suffering substantial detriment, including substantial distress **OR** Exposure of personal data of 10000+ users	Unauthorised access to/disclosure of sensitive personal data such as medical records or individuals working on animal research
Major	**EITHER** A potential or known breach of confidentiality where the release of data could cause a risk of individuals suffering substantial detriment, including substantial distress **OR** Exposure of personal data of 1000 – 10000 users	Unauthorised access to/disclosure of application data
Moderate	Exposure of limited personal data affecting 100 – 1000 users	List of user details (such as names and addresses) exposed (e.g. access to the Global Address List)
Minor	Exposure of limited personal data affecting < 100 users.	Unauthorised access to system containing limited, non-private information (e.g. usernames or email addresses.)

Financial Impact

Category	Description	Examples
Critical	Financial loss or impact exceeding £1m.	Example of financial impact could include fines or charges levied (e.g. non PCI compliance), loss of grant/funding income, cost of replacing systems, insurance premiums etc.
Major	Financial loss or impact of £100k - £1m.	
Moderate	Financial loss or impact of £20k - £100k	
Minor	Financial impact of < £20k	

Reputational Impact

Category	Description	Examples
Critical	EITHER sustained or ongoing negative national media publicity OR a negative change across all national or international HE sector rankings	Significant data breach, compromise or unavailability of critical University system; Compromise of major and/or sensitive research project
Major	EITHER one-off negative national, or ongoing local, media publicity OR a negative change across the majority of national or international HE sector rankings	Compromise of non-critical but high-profile system
Moderate	EITHER negative media publicity likely, but avoidable or controllable with management OR a negative view of individual departments at Council level	Loss or theft of unencrypted laptops containing confidential information.
Minor	Negative view limited to within a department	Incident affecting limited number of users within a single department.

Incident classification

Having been assigned an overall category and given an impact score, incidents will then be classified according to the following criteria:

Emergency (Class 1)	Critical information system is affected **AND** Results in critical business, financial, reputational or information impact.
Critical (Class 2)	Critical or major information system is affected **AND** results in Major business, financial, reputational or information impact; **OR** Results in critical business, financial or reputational impact.
Major (Class 3)	Major or moderate information system is affected **AND** results in moderate business, financial, reputational or information impact; **OR** Results in Major business, financial, reputational or information impact
Minor (Class 4)	Moderate or minor information systems affected AND results in minor business, financial, reputational or information impact; **OR** Results in Moderate business, financial, reputational impact

Appendix B: Information required by the Data Protection Officer for incidents involving personal data

The following questions will be used as the basis for investigating information security incidents involving personal data. This reflects the information that the Data Protection Officer will need to ascertain in order to make a decision on whether to pursue the incident and potentially report to the Information Commissioner's Office.

1. What is the full range of data exposed
2. What is the nature of the data (personal, sensitive personal etc.)
3. What is the quantity/volume/number of users affected
4. What is the evidence of data having been being exposed and what is the nature of the exposure (i.e. data already in the public domain, data exposed but unlikely to be the target of the attack/incident etc.)
5. For how long has the data been stored/kept
6. Is the data still current i.e. for how long should it have been stored/kept
7. What measures were in place to protect the data
8. Have any complaints been received
9. Was the attack specifically targeted/what was the likely motivation of the attack
10. What was the cause/vulnerability
11. What measures have been put in place to mitigate

Appendix C: Escalation and Reporting of Incidents

Class 4 incidents usually require no escalation. Records of the incident will be maintained for statistical purposes by the ISIRT. Where appropriate further investigations will take place by the ISIRT team to ascertain whether the incident needs to be escalated and/or the extent to which personal (or otherwise confidential) data is involved. Where personal data is involved a report will be provided to the Data Protection Officer

Statistics of all Class 4 incidents will be reported at ISAG meetings.

Class 3 incidents will be escalated to the the Director of IT Risk Management who will make a judgement as to whether further investigation is required. Incidents will normally not need to be escalated immediately but the Director of IT Risk management will ultimately be informed of all such incidents. Where personal information is involved the ISIRT will carry out initial investigations into the nature and extent of the information and the exposure, before sending a report of the incident to the Data Protection Officer.

Statistics of all Class 3 incidents will be reported at Information Security Working Group meetings.

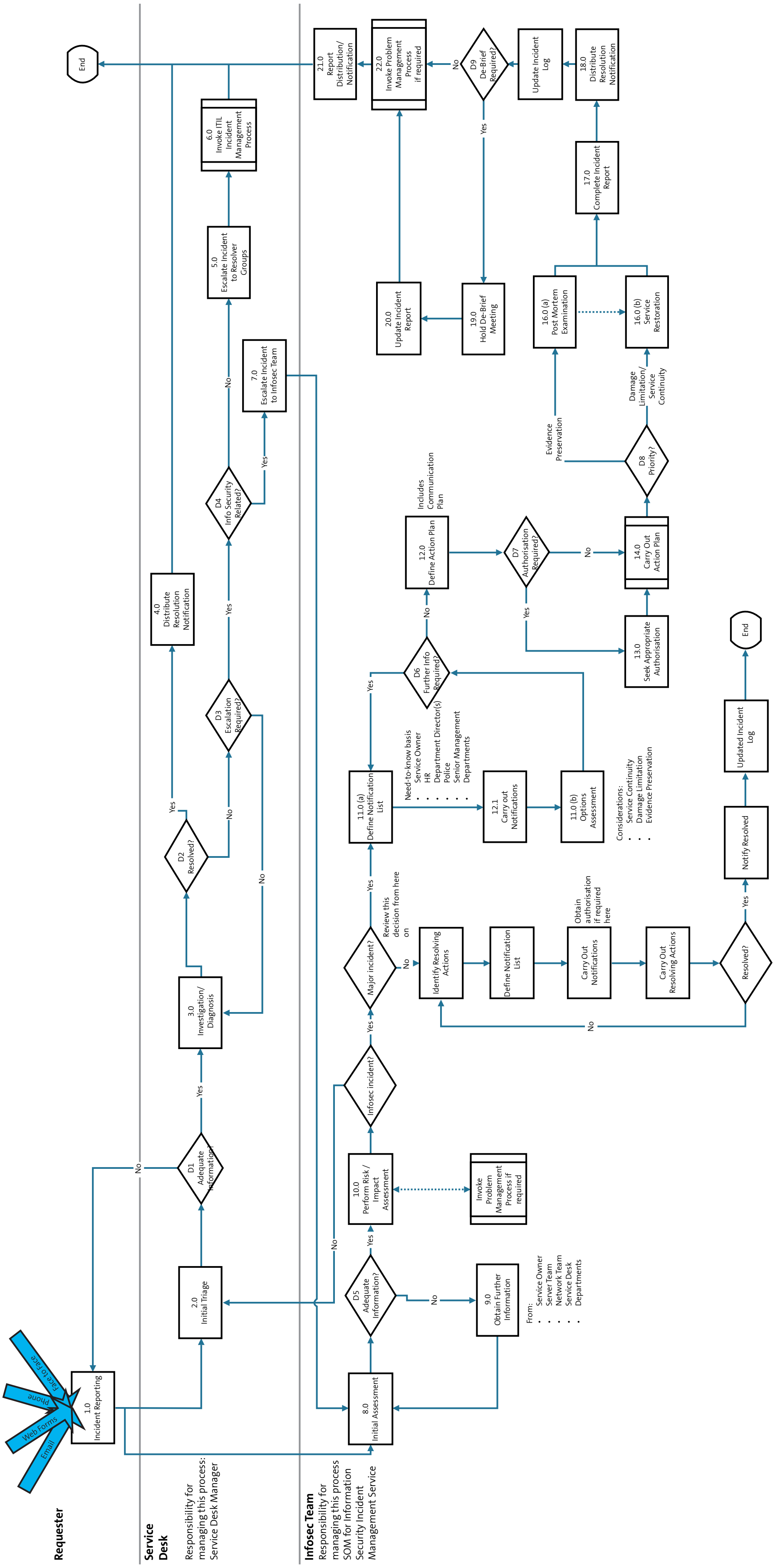
Class 2 incidents will be escalated immediately to the Director of IT Risk Management and Head, Head of Compliance and, where personal data is potentially involved, the Data Protection Officer. The ISIRT will still usually be responsible for the initial investigations into the nature and extent of exposure of any personal information but the Data Protection Officer will likely be involved in all communications.

Class 2 incidents, including their handling, eventual impact and lessons learned, will be reviewed at ISAG meetings.

Class 1 incidents will be escalated immediately to the whole crisis/escalation team. The CIO, Head of Compliance and Director of IT Risk Management will be responsible for coordinating the response to such incidents, ensuring sufficient resources are allocated to dealing with the incident and for keeping senior stakeholders (such as the Registrar) fully informed.

Class 1 incidents, including their handling, eventual impact and lessons learned, will be reviewed at Information Security Working Group meetings.

Information Security Service: Information Security Incident Management Process – UCL


Requester
Face to Face
Phone
Web Forms
Email
1.0 Incident Reporting
End
Service Desk
Responsibility for managing this process: Service Desk Manager
2.0 Initial Triage
D1 Adequate Information?
No
Yes
3.0 Investigation/ Diagnosis
D2 Resolved?
Yes
No
4.0 Distribute Resolution Notification
D3 Escalation Required?
No
Yes
No
D4 Info Security Related?
Yes
No
5.0 Escalate Incident to Resolver Groups
6.0 Invoke ITIL Incident Management Process
7.0 Escalate Incident to Infosec Team
Infosec Team
Responsibility for managing this process SOM for Information Security Incident Management Service
8.0 Initial Assessment
D5 Adequate Information?
No
Yes
9.0 Obtain Further Information
From:
Service Owner
Server Team
Network Team
Service Desk
Departments
No
10.0 Perform Risk / Impact Assessment
Invoke Problem Management Process if required
Infosec incident?
Yes
Major incident?
No
Yes
Review this decision from here on
Identify Resolving Actions
Define Notification List
Carry Out Notifications
Obtain authorisation if required here
Carry Out Resolving Actions
Resolved?
No
Yes
Notify Resolved
Updated Incident Log
End
11.0 (a) Define Notification List
Need-to-know basis
Service Owner
HR
Department Director(s)
Police
Senior Management
Departments
12.1 Carry out Notifications
11.0 (b) Options Assessment
Considerations:
Service Continuity
Damage Limitation
Evidence Preservation
D6 Further Info Required?
Yes
No
12.0 Define Action Plan
Includes Communication Plan
D7 Authorisation Required?
Yes
No
13.0 Seek Appropriate Authorisation
14.0 Carry Out Action Plan
D8 Priority?
Evidence Preservation
Damage Limitation/ Service Continuity
16.0 (a) Post Mortem Examination
16.0 (b) Service Restoration
17.0 Complete Incident Report
18.0 Distribute Resolution Notification
Update Incident Log
D9 De-Brief Required?
Yes
No
19.0 Hold De-Brief Meeting
20.0 Update Incident Report
22.0 Invoke Problem Management Process if required
21.0 Report Distribution/ Notification

Investigations and Data Access Policies – University of York, case study

An investigation policy can expect to be the most scrutinised documents in a whole policy suite. Investigations and Data Access policies will be used in circumstances ranging from access to documents of a member of staff off sick, to internal disciplinary procedures, to police requests for data and even requests for surveillance under warrant from the Home Secretary. As such, even more care and wide consultation are necessary that with other policies.

Different institutions will have different processes and expectations of privacy at work. At York, staff have always been permitted to use their work email accounts for personal use, we do not do web filtering and do not pro-actively look at web logs for misuse. This culture of personal use and privacy affected the final policy in many ways, and was an explicit part of the initial discussions. Other institutions may take a very different line: FE institutions will usually have web filtering and altering for example.

These differences in emphasis mean that it is very unlikely that any general document will work, and a policy tailored to the institution will be necessary.

At the University of York our previous policy was very old and no longer fit for purpose. The title itself was a problem: "Policy for Investigation of Incidents under the Regulation of Investigatory Powers Act" seemed to imply that the policy only applied RIPA requests, and not for anything else, when we used it not just for other legal requests but also for internal investigations.

The policy had other serious issues as well:

- It did not mandate record keeping
- It did not prescribe what to do if illegal material might be found
- It made promises we could not keep about what might happen in court cases
- There was no clear demarcation between who could authorise a request and who could do the work. A Head of Department could both initiate and authorise an investigation
- It pre-dated the use of cloud services. It was possible to read it so that cloud services came into scope, but it was also possible to argue that they did not. With the University of York adopting Google Apps this became an urgent problem.

It was very obvious that the old policy did not just need a minor update, so we started again from scratch.

We came up with a set of sample issues and scenarios based on real cases over the past few years, and thought about how the old policy had made life difficult. This generated a list of areas we needed to fix. Next we looked at how within the University should authorise requests. We were surprised at the difference in views here: some departments thought that line managers (at any grade) should be able to authorise access, others wanted it limited to very senior staff and it was important to get agreement on this fundamental principle before other work was done.

We also listed our constraints and assumptions. This helped us to consider specific parts of the policy against criteria and was helpful when "lost in the detail". For example:

- The policy had to align with other policies such as social media policy
- We needed to consult with unions etc.
- None of our staff are trained to evidence standards and the University had no wish to establish a forensics facility
- We assumed that users would be informed about access unless there was a specific reason not to do so
- We wanted the scope of the data accessed to be drawn as tightly as possible
- To protect privacy, we do not normally give direct access to an account (either via sharing the password or delegation), instead we pass on the data.

Our final policy has been in place for a year, and works for us. It protects University members' privacy by requiring sign off at a senior level (Head of Department for internal requests, the Registrar for external legal ones) and ensuring separation of request and authorisation but still allows us to quickly give access to data in situations where it is urgent.

Links to policy

Policy
http://www.york.ac.uk/media/abouttheuniversity/supportservices/informationdirectorate/documents/policies/ITInvestigationsandDataAccessPolicy_Oct2013.pdf

Method Statement
http://www.york.ac.uk/media/abouttheuniversity/supportservices/informationdirectorate/documents/policies/MethodStatement-InvestigationsandDataAccess.pdf

Proforma (Word document) on the web page
http://www.york.ac.uk/about/departments/support-and-admin/information-directorate/information-policy/

Data breach – case study

The University of Morpeth is a research intensive pre-92 University.

At 11.59 on a Friday night, CSIRT staff at the University of Morpeth were alerted via email that students had discovered a way to access a restricted system and could view personal information of moderate confidentiality by exploiting a mis-configuration in a development system.

The message was picked up first thing on the Saturday morning, but due to a miscommunication between members of the team, the bug wasn't fixed until the Monday morning. Shortly after 9am on Monday the bug was fixed.

Because students had spotted the issue, the student press was in touch immediately, with other local media following later that day. University senior management were alerted while key technical staff set to work analysing the log files to understand the extent of the breach.

The University had not "war-gamed" an incident like this and the many decisions that have to be taken. For example, should a spokesperson be provided for TV/radio, or should all media enquiries just receive a prepared statement? Making such decisions required heavy levels of involvement from senior staff, working under considerable pressure. The University opted not to provide a case study for local radio and other requests, but kept this decision under close review as the incident progressed.

Fortunately, full logging was available and the University was able to determine every unauthorised access and which information was viewed. This proved to be key in managing the incident, with the certainty given by detailed logging helping to manage fears.

A key learning point is that any analysis needs to be communicated carefully: an initial estimate of the number of people affected was produced on the fly in a meeting by a member of the technical team. Within 90 minutes, and without double checking, that number was released in an official press release. Fortunately for everyone concerned, when double checked the next day, the number was correct.

Since the University now had a full list of the individuals affected, the nature of the data released and, in many cases, knowledge of who accessed the data, the decision was made to telephone everyone affected. Initial plans within IT had been to issue email alerts: the decision to telephone everyone affected by the breach proved a very good one. People contacted were surprised to be directly contacted, grateful for the chance to be reassured and get details on what happened.

To make this work, two key things were done. 1) All phone calls were done by two members of staff working in tandem and 2) a full script was written in advance covering opening lines, responses to questions, details of the insurance offered etc. The need for a script was contested by some staff, but its use in avoiding mistakes when making the 20th phone call of the day soon became apparent.

The combination of a formal response, transparency about the extent of the breach, personal communications and offers of suitable insurance seemed to work, with interest in the incident dropping rapidly after the first two days. There have been no reports of any loss or harm to individuals as a result of the incident.

In the aftermath of the breach, the Information Commissioner's Office was notified and a plan put in place to prevent a repeat including governance changes, staff training and changes to development practice.

Key points:

- Having an incident plan in advance, covering IT, Communications and University Senior Management with clear lines of escalation, out-of-hours contact details for key stakeholders and agreed criteria for actions e.g. when something is serious enough to place on the University's front page, can save a lot of time
- Develop a communication plan in advance
- Logs are vital, but manage the release of information internally as well as externally. Caveats around data get lost very rapidly.
- Personal communication with victims, if at all possible, is highly appreciated.
- Even with detailed communications to the media, some media organisations will get the facts very wrong. One on-line trade site reported a level of users affected two orders of magnitude too high! Such mistakes are had to correct and develop a life of their own. Getting the correct facts out as early as possible is the best defence.