Information Security Incident Management

1. Scope

1.1. This policy supplements the University’s information security policy. It applies to events and incidents affecting any University information asset or information system. The policy applies to all University information systems.

2. Objective

2.1. 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.

2.2. Compliance with the policy will ensure that:

   i. Incidents which are detected are reported in a timely manner
   ii. Incidents are properly investigated and handled efficiently and effectively
   iii. Incidents are communicated appropriately and appropriate levels of University management are involved in the response
   iv. The impact of an incident is minimized and action is taken to prevent further damage
   v. Incidents are reviewed to enable improvements to be made to policies and procedures
   vi. Evidence is gathered, recorded and maintained appropriately
   vii. Incidents are recorded and documented
   viii. External bodies or data subjects are informed as required

3. Policy

3.1. Information systems which are known to be compromised will be isolated from the University network until the incident has been investigated, resolved and risks sufficiently reduced.

3.2. Guidance and procedures for the detection, assessment, communication, reporting and escalation of security vulnerabilities, events and incidents will be provided via the information services webpages.

3.3. All information security incidents must be reported to irt@ed.ac.uk.
3.4. Responsibilities for the reporting and escalation of security vulnerabilities, events and incidents should be clearly defined.

3.5. Security events and incidents should be assessed according to the incident classification scheme provided via this document and, where necessary, escalated accordingly.

3.6. Incidents involving personal data will be reported to the University Data Protection Officer.

3.7. Incidents which involve personal safety, security or require the involvement of law enforcement will be reported to the Chief Security Officer.

3.8. Details of the Information Security Incident Response Plan will be made available via the information service webpages.

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

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

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

3.12. Technical support and guidance will be provided by IT Services and via the Information Services webpages and other, local, advice.

4. Incident Response Team (IRT)

4.1. The IRT 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 IRT consists of a ‘virtual team made up from members of the Comms Infrastructure and Unix groups of Information Technology Infrastructure (ITI) of Information Services. The roles and responsibilities for the IRT are as follows:

i. initial response, mitigation and (where appropriate) escalation of information security incidents

ii. monitoring network traffic to identify compromised or potentially compromised systems within the University network;

iii. Receiving internal and external reports on compromised systems

iv. Protecting the security and integrity of the University network and its core information systems and services by blocking network access to/from any compromised machine

v. Informing, liaising with, and supporting local IT staff to ensure that computer security incidents are dealt with promptly and effectively

vi. Coordinating with the User Services Division and local Computing Officers to ensure that compromised systems are fully cleaned and patched against known vulnerabilities, or the risk otherwise mitigated, before being reconnected to the network
vii. Providing advice and guidance on dealing with computer and network security via [http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations/security-policies](http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations/security-policies)
viii. Maintaining a record of computer security incidents processed by IRT
ix. Initial investigation and liaison with the service provider into the type and quantity of personal (or otherwise confidential) data involved in a compromise
x. Appropriate escalation of computer security incidents.

5. Escalation of Computer Security Incidents

5.1. Some incidents will require escalation above the IRT in order that senior management in the University are made aware of, and may respond accordingly, to serious and potentially serious information security incidents.

5.2. The first point of escalation for the IRT will be the Chief Information Technology Security Officer (CITSO) or in that person’s absence, the CIO. The role of the CITSO is described below.

5.3. The IRT will evaluate each security incident and will escalate the incident under one of the following conditions:

i. Any incident that causes a loss or impairment of a service
ii. Any incident that involves loss of sensitive information
iii. Any incident where University resources are used to attack other services or an external body

5.4. In the case of the loss of any personal information, the IRT will inform the Data Protection Officer and the CITSO of the incident.

6. Crisis/Escalation

6.1. In the case of a “most serious incident”, the CITSO will immediately inform the CIO of the incident and other senior University managers as appropriate.

6.2. The conditions under which this escalation will be performed are as follows:

i. Any incident which causes a major loss of service
ii. Any incident which may cause a major reputational risk
iii. Any incident that is a major loss of personal information

7. Reporting Security Incidents

7.1. Security incidents can be detected by various sources. All incidents must be reported either to the IRT team (irt@ed.ac.uk) or to the CITSO. In the case of a report to the CITSO the report will be passed to the IRT team for first line handling and logging.

7.2. The incidents are classified for reporting purposes using the Janet categories. A summary of these classifications are provided at the end of this document.
7.3. The current common sources of reports are the Janet CSIRT team, users or their Computing Officers, the helpline and internal monitoring tools.

7.4. The current common sources of reports to the CITSO are the data Protection Officer, School Computing Officers and the helpline.

7.5. In every case it is important that the incident is properly logged, the escalation procedure is evaluated and followed and the source of the incident is remediated.

8. Flow of Incident Reporting
9. **Role of the Chief Information Technology Security Officer (CITSO)**

9.1. The Chief Information Technology Security Officer, under the guidance of the Chief Information Officer (CIO), is responsible for:

i. The maintenance and communication of the incident response policy and scheme;

ii. Creating, maintaining and communicating the information security incident response scheme, incident classification scale and other relevant procedures and guidance via the information security policy;

iii. Receiving reports on information security incidents and breaches of the information security policy

iv. Appropriate escalation of information security incidents in accordance with the information security incident management policy

v. Reporting incidents involving personal data to the Data Protection Officer

vi. Maintaining and updating the information security register to reflect recorded incidents

vii. Writing and presenting appropriate incident reports to the Information Technology Committee, Risk management Committee, the Audit Committee and information systems/risk owners and including recommended remediations and lessons learnt.
Security Incident Classification Scheme

This scheme is derived directly from the Janet classification scheme and will be kept in step with that scheme.

**Compromise**

The more "traditional" security incidents get placed here. Systems that have been compromised through network service vulnerabilities, insecure passwords or web defacements usually end up in this category if one of the others is not more appropriate. These systems are often used to host illegal material, relay further attacks and access other systems, or to distribute malware. A judgment and distinction is made by the incident handler with systems that have been compromised through automated malware.

**Copyright**

Reports of copyright infringement.

**Denial of Service**

Attacks aimed at denying legitimate access to a network or service. These range from simply overwhelming a connection with greater traffic than it has capacity, to traffic especially crafted to consume CPU and memory resources on the target system.

**General Query**

An enquiry from a user, usually related to the provision of services by IRT.

**LEA**

Query/Enquiries from the police, or other law enforcement agency. This could include a request to obtain communications data under RIPA Section 22.

**Legal/Policy Query**

An enquiry from a user on a legal or policy issue.

**Malware**

An incident that primarily involves a system being infected with malicious software without the user's consent. The overwhelming majority of these incidents will naturally be due to large outbreaks of malware, but they can range from targeted attacks to banking Trojans.
**Network Security Query**

An enquiry from a user about best practices in network or information security.

**Other**

Anything that does not fall into one of the other categories.

**Phishing**

Incidents involving phishing e-mails being sent to or received from a user. The overwhelming majority of these are low level unsophisticated phishing attacks designed to capture e-mail account details for use in advance-fee fraud. More sophisticated attacks often cross into the malware category.

**Scanning**

Count of non-trivial attempts by external systems to scan our network for vulnerabilities.

**Social Engineering**

Attacks where information or access to systems is obtained through the deception of people. Since we split phishing from this category, very few incidents are now classified here.

**Unauthorised Use**

Misuse of our network, not covered by other categories, as defined by our AUP and Security Policy.

**Unsolicited Bulk Email**

Spam sent from our systems.