Information Security Incident Management Procedure

Incident Reporting, Management, and Consequence Management Procedures

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document control

Superseded documents

Version history

Version	Date	Comments
0.1	18 Nov 2016	First draft
0.2	09 Dec 2016	Updates and corrections from Information Access Officer
0.3	13 Dec 2016	Correction to job Title Head of IS Infrastructure & Operations.
1.0	06 Apr 2017	Approved by Exec
1.1	20 Nov 2018	Correction to Job Titles

Outstanding issues and omissions

Issue control

Owner:	Cyber & Information Security Manager
Signature:	Date:
Approver:	Chief Information Security Officer
Signature:	Date:
Distribution:	

ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A16 – Information security incident management
ISO 27001:2013 Conformance Control	Information Classification Objective A.16.1 - Management of information security incidents and improvements

1.0 Contents:

2.0 Cyber & InfoSec Incident Management System

2.1 Introduction

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

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

Please refer to BUL-GLOS-000 - SyOPs for the glossary of terms, acronyms and their definitions for the suite of BUL ISMS documentations.

2.2 Cyber & Information Security Incident Management Procedure

Scope

This procedure forms part of the information Security Management System (ISMS) framework and supplements the University's Information Security Policy (ISP) and BUL-POL-16.1 Infosec Incident Management Policy. It applies to events and incidents affecting any University information assets or information systems. It applies to and will be communicated to all those with access to University information systems, including staff, students, visitors and contractors.

This procedure applies to:

- all information created or received by the University in any format, whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;
- all staff and students, affiliates or contractors working for or on behalf of the University and any other person permitted to have access to University information;
- all University IT systems managed by IS, Colleges and Institutes;
- any other IT systems on which University information is held or processed.

An *information security incident* is 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, electronic data, or equipment such as tablets, laptops and smartphones on which data is stored
- Inappropriate access controls allowing unauthorised use of information
- Suspected breach of the University IT and communications use policies (Brunel Acceptable Use Policy (BACUP), Electronic mail policy, Network Account 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
- Social Engineering or the manipulation of an individual to impart confidential information 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 or inadequate review of access rights
- 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

2.3 Objectives

By complying with these procedures the University will benefit by:

- Effectively managing security incidents;
- Identifying measures which will avoid reoccurrence of the incident;
- Ensuring security needs are appropriately addressed;
- Increasing the security of Brunel University London assets.

It is not about apportioning blame to an individual (unless there is evidence of a deliberate failure to comply with Brunel University London security policies or actions of fraud, corruption, dishonesty, illegal or reckless behavior, etc.); instead, failure to report a security incident may leave the system, building and/or individual open and vulnerable to increased risk, including personal safety in the case of individuals. Therefore you must report all actual and/or attempted breaches of security.

All security incidents, whether suspected or actual, must be reported to your Line Manager, the Cyber & Information Security Manager and/or site Head of Security (HoS). The Cyber & Information Security Manager is responsible for reporting all incidents to the HoS and Computer Security Incident Response Team (CSIRT**)** team and the as soon as operationally possible.

Unless specifically instructed by an authorised individual (i.e. Cyber & Information Security Manager, IT Manager, CSIRT, HoS etc.) you must not touch, interfere with (i.e. examine) or allow unqualified or unauthorized individuals to touch or investigate electronic equipment or devices. To do so could result in the loss or corruption of information or subsequent damage to equipment and/or evidence.

Unless specifically instructed by an authorised individual (i.e. Cyber & Information Security Manager, IT Manager, CSIRT, HoS etc.) you must not disconnect power sources, including batteries. To do so may result in the loss of Random Access Memory (RAM).

All incidents remain open until they have been investigated, reported and rectified in accordance with agreed corrective actions.

2.4 Information Security Incidents and Information Security Events

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

Cyber & Information security events are described as:

- Identified occurrences of systems, services or networks that have the potential to breach information security policies, or are recognised as occurrences, or tactics used by adversaries attempting to compromise confidentiality, integrity, or availability of information assets.

Cyber & 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 in Table 1:

Table 1

Cyber & Information security events	Cyber & Information Security incidents
Network scanning Brute force attempts/multiple login attempts Unsuccessful SQL injection attacks Human errors	Lost or stolen laptops or mobile devices Server compromises Botnet infections Successful SQL (or other code) injection attacks Compromised accounts (e.g. accounts spamming) Denial of Service attacks Unauthorised access to information systems Data breaches, lapses or contraventions Information security breaches, lapses or contraventions Someone has access to your account using your username and password – Compromised account Files are missing from your home directory, or files have been changed without your knowledge A virus infection that was not detected and cleaned automatically Someone gaining access to a building or part of a building who should not have access Theft of information or equipment Loss of service, functionality, equipment or other facilities System, software or hardware malfunctions, unscheduled shut downs, unexpected system errors or overloads Non-compliances with requirements of the ISMS (including uncontrolled system changes) Access violations

3.0 Lines of Responsibility

All users who are given access to University information, IT and communications facilities are responsible for reporting any actual or potential breach of information security promptly in line with the incident management procedures.

3.1 Cyber & Information Security Incident Response Team (IRT)

The IRT refers to the group of people who, at the Bronze levels, will act as the first responders to deal with a cyber & information security incident. It will be dependent on the nature of the incident as to which part of the IRT leads for example, IT related, INFOSEC related, or Data Protection related. The roles and responsibilities for the Bronze IMT are as follows:

3.1.1 Computer Security Incident Response Team (CSIRT)

The CSIRT are members of the IT staff on standby to deal with Cyber & INFOSEC incident management under the responsibility of the Head of IT Infrastructure & Operations.
They 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;
- Providing advice and guidance on dealing with computer and network security;
- Maintaining a register of computer security incidents;
- Where personal data has been exposed, escalating the incident to the Information Access Officer to provide the 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 cyber & information security incident management plan.

3.1.2 Cyber & Information Security Manager

The Cyber & Information Security Manager is responsible for:

- Coordination of the IMT and SILVER lead with regards to incident response;
- The maintenance and communication of the incident response policy and scheme;
- Creating, maintaining and communicating the information security incident response plan, incident classification scale and other relevant procedures and guidance;
- Coordination of University-wide responses to cyber & information security incidents via the IMT escalation team;
- Receiving and maintaining reports on information security incidents and breaches of the information security policy;
- Appropriate escalation of information security incidents in accordance with the cyber & information security incident management scheme/plan;

- Reporting incidents involving personal data to the Information Access 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 Cyber & Information Security Steering Group and information systems/risk owners and including recommended remediation and lessons identified.

3.1.3 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 Cyber & information security manager & Head of Security;
- Appropriate escalation of information security incidents in accordance with the cyber & information security incident management scheme/plan;
- Decisions to report, and subsequent reporting of, data protection incidents to the Information Commissioner;
- Reporting incidents to the Cyber and Information Security Manager;
- Communication to relevant staff of correspondence with the Information Commissioner

3.2 Crisis & Escalation – Incident Management Team (IMT) – Gold / Silver Levels

Some incidents will require escalation above the CSIRT in order that senior management within the University at the IMP[1] at the Gold & Silver levels are made aware of, and may respond accordingly to, serious and potentially serious cyber & information security incidents. The IMT consists of senior members of relevant University departments. Not all members of the IMT will need to be alerted to all cyber & information security incidents immediately. The classification scheme and requirements for escalation set out below will be used by the CSIRT to determine when the various parts of the IMT will be notified and stood up for managerial oversight and action.

The IMT is stood up by the SILVER lead (HoS) at the point of an incident and comprises those roles required to deal with the incident management and enduring consequence management. The IMT will be responsible for the resolution of the incident, business continuity, and consequence management.

The IMT will be made up of a core set of IMP senior staff and may therefore consist of but is not limited to:

- COO (as required) – Gold
- CIO (Chair) – Gold Incident Officer
- CISO – Gold incident officer
- Head of IT Infrastructure & Operations– Gold Incident Support Officer
- Cyber & InfoSec Manager – Silver incident support officer

[1] University Wide Incident Management Plan

- Network & Systems Managers – Silver incident support officers
- Data Protection Officer – Silver incident support officer

Additionally other key stakeholders will need to be informed, consulted and respond as appropriate. It will be the responsibility of the SILVER incident officer, as per IMP, to report to relevant stakeholders and increase the support team for incident officers appropriately. These stakeholders include but are not limited to:

- Press Officers
- Directors of College Operations / Research Operations
- Registrar & Director Student Services
- HR
- Governance, Information & Legal Office (GILO)

Roles and Responsibilities for the IMT

The roles and responsibilities for the Cyber & INFOSEC IMT are as follows:

3.2.1 CIO

- Acting as the senior GOLD incident officer for Cyber & INFOSEC incidents – reporting to the GOLD lead as appropriate (COO)
- Receiving reports of incidents that have been escalated and confirming the classification of those incidents
- Advising on and authorising mitigating actions and responses that either have a direct or indirect effect on the Computer Centre, or that the Computer Centre will implement but may have considerable implications for other departments and/or the University
- Providing senior management support for the IMT and Gold Incident Officer and the incident response scheme.
- Warning and Informing consequence management & business continuity impact as required to COO and VC.

3.2.2 Chief Information Security Officer

- Receiving reports of incidents that have been escalated and confirming the classification of those incidents;
- Warning and Informing the key senior Gold and Silver stakeholders such as the Registrar, Press Office, GILO, HR, Directors of College Operations and any other relevant senior stakeholders so they are fully informed and updated on the progression of incidents as appropriate;
- Providing senior Cyber & INFOSEC management support for the incident response teams;
- Decisions to report information security incidents to law enforcement;
- Responding to physical security issues as a result of information security incidents;
- Overseeing major investigations into breaches, lapses or contraventions.

3.2.3 Head of IT Infrastructure & Operations

The Head of IT Infrastructure & Operations is specifically responsible for:

- The overarching management of the CSIRT capability & authorising corrective actions to be taken by the CSIRT;

- Overseeing, measuring and monitoring the performance of the CSIRT and incident response team;
- Providing senior support and seeking sufficient resource in order to successfully implement and maintain the CSIRT & IT related incident response teams;
- Ensuring incidents are escalated appropriately to other 'stood up' members of the IMT;
- Leading the coordination and response of the IT elements of the IRT.

4.0 Reporting Security Incidents

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

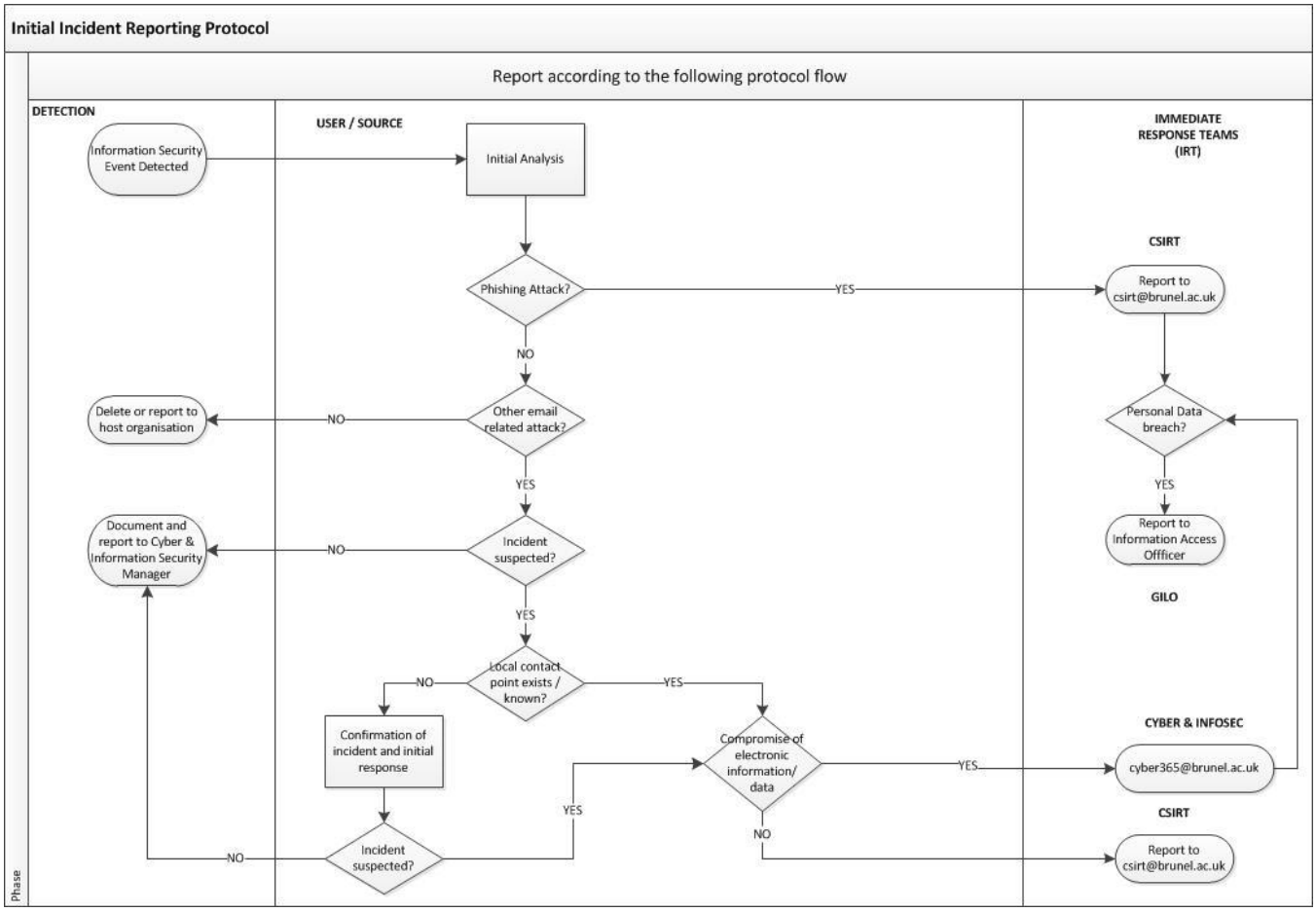
Cyber & information security **incidents** and weaknesses are reported immediately they are seen or experienced.

All Cyber & Information security **incidents** must be reported. The University operates a devolved model for support when it comes to IT and Cyber & information security, therefore users should usually report security incidents to identified local contacts for cascade. 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. Cyber & Information security incidents should then be reported according to the initial incident reporting protocol described below.

Cyber & information security **events** need not be reported immediately but **may** be reported periodically for information purposes. Cyber & 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 Cyber & 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 Cyber & information security events unless specific problems are identified.

Initial Incident Reporting Protocol

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



Central Incident Response and Escalation

The CSIRT 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 Information Access 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 to 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 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 IMT the information they require to determine what (if any) action is required; incident escalation reports will include the following information:

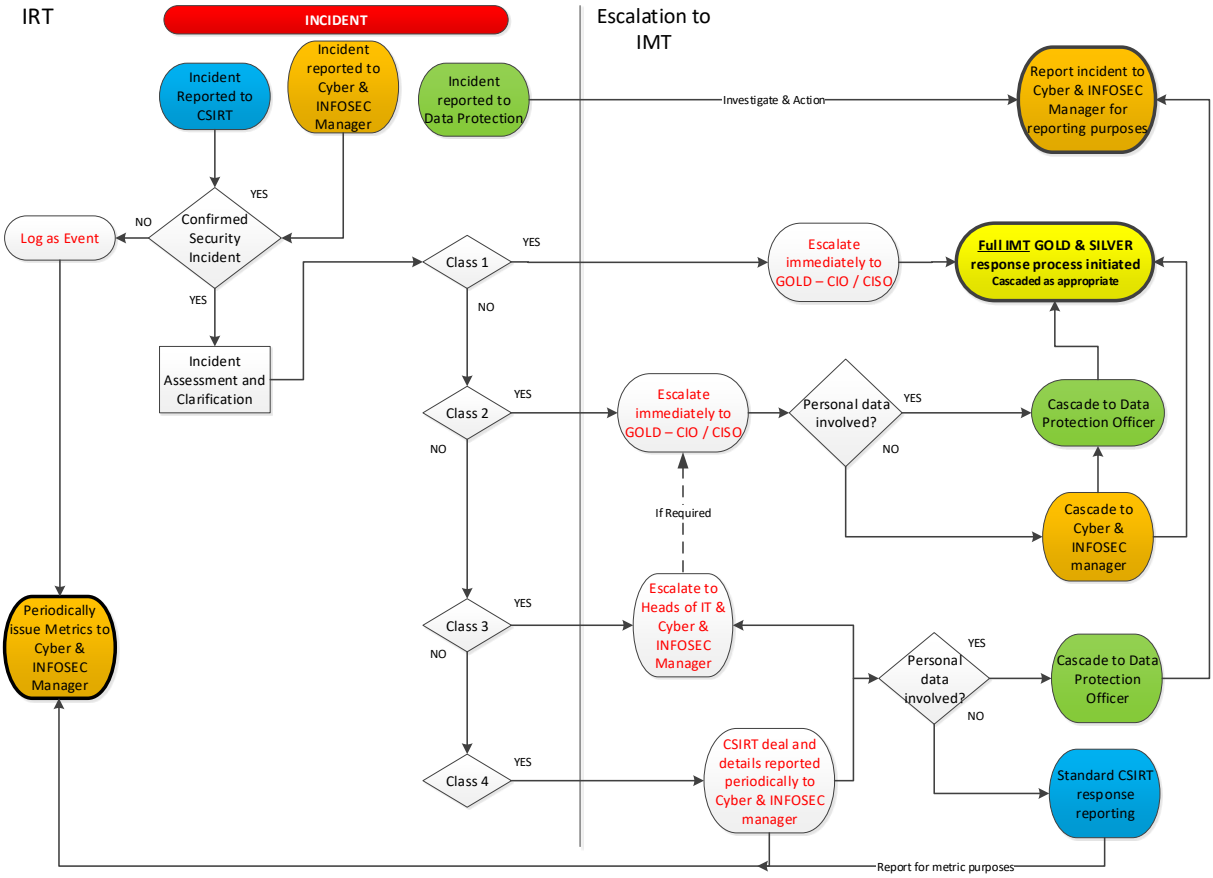
- Suspected date/time of incident
- Detection date/time
- Method of detection
- Incident category
- Current incident classification
- Basis for current classification
- Current status of investigation
- Current mitigating actions
- Potential incident classification
- Basis for potential incident classification (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 IMT

Updates to the status of an incident will be provided by the CSIRT either in accordance with the IMT 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 IRT in accordance with the protocol described below:



5.0 Crisis/Escalation Process

When cyber & information security incidents are escalated one person should take overall responsibility for coordinating the crisis response and incident resolution. This will be the Head of IT Infrastructure & Operations for IT related incidents. The lead coordinator will be responsible for ensuring the IRT provide updates as appropriate and will be responsible for overseeing and authorising responsive action (including meetings of the IRT, further escalation and eventually resolution of the incident. All members of the IMT have the responsibilities outlined above and are responsible for requesting relevant information for their area of responsibility.

5.1 Escalation of Information Security Incidents

All information security incidents will be reported at the university committee and executive board meetings and it is the responsibility of the CISO and Cyber & INFOSEC manager to ensure that incidents are presented and reported appropriately to these groups.

Class 3 and Class 4 incidents will be reported statistically to the information subcommittee meetings 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 and presented to Executive Board. Further details are presented in Appendix C.

6.0 Feedback

To complete the Security Incident Management and Reporting Process the investigating representative will complete and sign the Security Incident Report and return it to the IRT for closure of the incident.

7.0 Review Process

Following the completed investigation of an incident, a review must be carried out to assess how the incident was handled and to identify any 'lessons learnt'. This will help to prevent a similar incident or the reoccurrence of the original incident happening, as well as to identify any additional measures required to try and prevent future incidents, etc., the security incident reporting form will be essential in this process.

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, unsupported/end of life (EOL) or out of support infrastructure, 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 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 realised).

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**	Unauthorised access to/disclosure of sensitive personal data such as medical records or individuals working on animal research

	Exposure of personal data of 10000+ users	
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 or data breach comprises aggregation of an individual's data or includes Personal Sensitive data	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 unless the aggregation of an individual's data or Personal Sensitive data has been exposed.	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 Information Access Officer will need 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 CSIRT /IRT. Where appropriate further investigations will take place by the CSIRT / IRT 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 Information Subcommittee meetings and captured statistically on all security and emergency management reports into the relevant committees & Exec board.

- **Class 3** incidents will be escalated to the CISO who will make a judgement as to what type of further investigation or forensics are required. Incidents will normally not need to be escalated immediately but the Head of IT Infrastructure & Operations will ultimately inform the CISO of all such incidents. Where personal information is involved the IRT 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 & CISO. Statistics of all Class 3 incidents will be reported at Information Subcommittee meetings and captured statistically on all security and emergency management reports into the relevant committees & Exec board.

- **Class 2** incidents will be escalated immediately to the Head of IT Infrastructure & Operations, CIO, and CISO and, where personal data is potentially involved, the Data Protection Officer. The IRT 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 info subcommittee meetings. All such incidents will be reported at SG meetings and captured statistically on all security and emergency management reports into the relevant committees & Exec board

- **Class 1** incidents will be escalated immediately to the whole IMT and inform cascade channels. The CIO, CISO, Head of IT Infrastructure & Operations, will be responsible for coordinating the response to such incidents, ensuring sufficient resources are allocated to dealing with the incident and for keeping all senior stakeholders fully informed.

  Class 1 incidents, including their handling, eventual impact and lessons learned, will be reviewed at all info subcommittee meetings. All such incidents will be reported at SG meetings and captured statistically on all security and emergency management reports into the relevant committees & Exec board.

Appendix D: Cyber Security Incident Reporting Form

Important Note: This Security Incident Report from must be used for reporting all Cyber and InfoSec related security incidents in keeping with the ISMS Information Security Incident Management Procedure and the ISMS Information Security Incident Management Reporting Procedures. . The completed form must be forwarded to the Head of Security and Emergency Planning and the Chief Information Officer immediately after the Incident has been discovered and investigated. When completed this document becomes a **UNIVERSITY CONFIDENTIAL** document.

Section 1: Mandatory Information Requirement		**Reference Number:**	
Name of person reporting incident:		**Location:**	
Job Title (if applicable):		**College / Department:**	
Location of Incident:		**Date & Time of Incident:**	
Date reported to CSIRT / IT:		**Time reported to CSIRT / IT:**	
Impact Category:	Minor Class 1	**Incident Category:**	Other incidents

Section 2: IT Incidents

2.1	**Full Details of IT Incident** (any equipment affected, when and how the incident was discovered and effect on system or service, details of all other parties; including 3rd parties))
2.2	**Full details of interim actions and permanent actions to remedy the incident** (all steps that were taken and needs to be taken to resolve the cyber security incident and to prevent it from reoccurring

2.3	**Feedback regarding the incident** (to complete and sign. Please return to the Head of Security and Emergency Planning and the Chief Information Officer)
2.4	**Post Incident Assessments:**

Sign off by Assessors	Head of Security and Emergency Planning	Cyber and Information Security Manager
Name (block capitals)		
Signature:		
Date:		

Distribution:

Secretary to Council & University Secretary
COO
CIO
CISO
Head of IT Infrastructure & Operations
Academic Registrar & Director Student Services
Asst. Director Commercial Services – Fac & Ops
IT Systems Manager
Data Protection Officer
Head of Security