University of Liverpool

Information Security Incident Response Policy

Reference Number	CSD-012
Title	Information Security Incident Response Policy
Version Number	1.2
Document Status	Active
Document Classification	Open
Effective Date	22 May 2014
Review Date	28 March 2018
Author	Computing Services Department (David Hill)
Approved by	Corporate Services & Facilities Committee (Nov 2012)
Implemented by	Information Security Officer
Monitoring of compliance	Faculty Information Security Managers (Local) CSD Information Security (Central)
Comments	• **22/05/2014 - Annual Review/Update v1.0 – v1.1** • **31/07/2015 – Annual Review/Update v1.1 – v1.2** • **29/07/2016 – Annual Review** • **28/03/2017 – Annual Review**

Information Security Incident Response Policy

1. Introduction

Information is a vital asset to any organisation, and this is especially so in the University which is a knowledge-driven organisation. Virtually all of our activities create information assets in one form or another. The Information Security Incident Response Policy and its associated policies are concerned with managing the information assets owned by the University and used by staff/student(s) of the University in their official capacities.

2. Principles

The Information Security Incident Response Policy specifies a repeatable methodology which defines the roles and responsibilities staff/student(s) have when dealing with a security incident. The University has adopted the following principles, which underpin this policy:

- All information assets must be appropriately handled and managed in accordance with their classification.
- University information assets should be made available to all who have a legitimate need for them.
- The integrity of information must be maintained; information must also be accurate, complete, timely and consistent with other related information and events.
- All staff/student(s) of the University, who have access to information assets, have a responsibility to handle them appropriately and in accordance with their classification.
- Information Asset owners are responsible for ensuring that the University classification scheme, which is described in the Information Security Policy, is used appropriately.

3. Objectives of this Policy

- To define appropriate mechanisms for responding to different security incidents
- To ensure that asset owners are appropriately identified and have been informed of security incidents
- To assign responsibilities for the security incident response management process
- To ascertain the seriousness and the extent of damage of an incident
- To identify any vulnerabilities created
- To estimate what resources are required to mitigate the incident
- To ensure that proper follow-up reporting occurs and that procedures are reviewed and adjusted in order to mitigate risks and to establish appropriate actions to prevent future incidents.

4. Action Implementation

Procedures will be put in place in order to ensure effective security incident management; the objectives of those procedures will be:

- To ensure that security incidents are reported to the relevant sources.
- To define the roles and responsibilities of the University
- To co-ordinate and oversee the response to Incidents in accordance with the requirements of UK legislation and University policies.
- To minimise the potential negative impact to the University, its customers and third parties as a result of such incidents.
- To inform, where appropriate, the affected customer and/or third party of action that is recommended or required on their behalf.
- To restore services to a normal and secure state of operation in a timely manner.

- To provide clear and timely communication to all relevant parties.

5. Security Incident Management

All Security incidents must be reported to the relevant University contacts immediately.

Detecting Information Security Incidents

University staff must ensure that University assets are appropriately protected. The steps needed to accomplish this will include:

- Compliance and Monitoring (Manual or Systematic reporting)
- Proactive threat discovery e.g. system and network monitoring of current and new threats
- Intrusion Detection and Prevention
- Vulnerability Prevention and Scanning
- Root Cause Analysis

***The above list does not cover all threats and vulnerabilities against the University and is reliant upon any visible and suspicious activity that is witnessed or detected being reported accordingly.**

Different Types of Information Security Incidents

For the purpose of this policy - *"Information security incidents can be accidental or malicious actions or events that have the potential to have unwanted effects on the confidentiality, integrity and availability of University information and IT assets*".

Examples of information security events and incidents that may pose a threat to the University and its information assets include:

- Presence of unauthorised personnel in sensitive areas/buildings
- Secure or sensitive storage areas found unsecured (includes delivery points)
- Theft or physical loss of University information assets (electronic/non-electronic information assets) known to have sensitive information associated (e.g. laptops/mobile phones)
- Loss of storage media (removable drive, CD, DVD, flash drive,)
- A server known to hold sensitive data which has been accessed or otherwise compromised by an unauthorised entity
- Suspicious or foreign hardware connected to the University's data network
- An outside entity which is subjected to attacks originating from within the University's data network
- An unauthorised or unwarranted entity causing a network outage
- System slowdown or failure
- Changes in default or user-defined settings
- Unexplained or unexpected use of system resources
- Unusual activities appearing in system or audit logs
- Changes to or appearance of new system files
- Users unexpectedly locked out
- Appliance or equipment failure
- Unexpected enabling or activation of services or ports
- Unexpected activity that has been detected by the University's security defences. For example, this might include unusual patterns of attack detected by the University firewall.

6. University Security Services (Physical Security)

Breaches of physical security must be reported to the University Security Services. Examples of these types of breaches include:

- Presence of unauthorised access in sensitive areas/buildings/comms rooms
- Secure or sensitive storage areas found unsecured (includes delivery points)
- Risks to National Security, the University and its staff/student (s) e.g. threatening calls, terrorism threats and threatening emails from external resources.

University Security Services Contacts and Service times

For key contacts and service times for the University Security Services please refer to http://www.liv.ac.uk/facilities-management/key-contacts/#d.en.144373

7. Reporting Information Security events/incident(s)

Dependent on the type of information security incidents and events, staff/student(s) must report them to one of the following staff members and teams to ensure that any risks can be addressed and mitigated accordingly:

- Line Manager/Faculty Security Manager
- CSD SIRT (Security Incident Response team)
- CSD Service Desk

Line Manager/Faculty Security Manager

You should report information security incidents that are sensitive in nature/user specific to your line manager and/or faculty Security Manager in the first instance. The line manager/faculty security manager will then liaise with the Security Incident Response Team (SIRT).

CSD Security Incident Response Team (SIRT)

If a security incident requires immediate CSD involvement then it should be reported to the relevant SIRT members directly (risk and nature dependent). For the purposes of this policy, the SIRT is associated to a role and not an individual. The SIRT team consist of:

Director of Computing Services
Deputy Director of Computing Services
Head of Customer Services
Head of Infrastructure Services
Head of Business Information Systems & Services
Head of Application System and Services
Information Security Officer

CSD Service Desk

The CSD Service Desk is a central point of contact (POC) where staff/student(s) of the University can contact to report an Information security event or incident. The CSD Service Desk can help the staff/student(s) to determine the initial prognosis and acknowledge if the scenario witnessed is an actual Information security event /incident or if there are other issues which are causing the problem.

In the event of an actual information security incident the CSD Service Desk will contact the relevant SIRT members accordingly.

Summary of Information Security Incident Notification Channels

<table>
<tr><th colspan="4">Information Security Incident Type and Notification Channels</th></tr>
<tr><td colspan="2">Isolated/Sensitive Nature</td><td colspan="2">University Wide/Non Sensitive/CSD Managed Services</td></tr>
<tr><td colspan="2">• An investigation of the behaviour of a staff/student(s).
• Accessing, storing, sending or creating illegal content via University IT Assets including: PCs, Networks, email facilities and storage facilities.
• Accessing, storing, sending or creating illegal activity whereby National Security and the University and its staff/student(s) may be at risk.
• Accessing, storing, sending or creating abusive content that may cause distress.</td><td colspan="2">• Network outage(s)
• Appliance or equipment failure
• Theft, loss and destruction of University IT Assets (PC/Laptop/Mobile Phone)
• Unexplained or unexpected use of system resources
• System slowdown or failure
• Protective mechanisms disabled (firewall, anti-virus)</td></tr>
<tr><th colspan="4">Initial Notification(s)</th></tr>
<tr><td>Staff/Student(s)</td><td>Academic/Line Manager</td><td>Staff/Student(s)</td><td>Academic/Line Manger</td></tr>
<tr><td>Academic/Line Manager</td><td>Faculty Security Manager</td><td>Academic/Line Manager</td><td>CSD Service Desk</td></tr>
<tr><td>Faculty Security Manager</td><td>CSD SIRT</td><td colspan="2"></td></tr>
</table>

N.B In the event your line manager is unavailable - University Wide/MWS Incidents must be reported directly to the CSD Service Desk.

CSD Service Desk Contacts and Service times

Staff/student(s) of the University can raise information security incidents via:

- Logging an online support request: http://servicedesk.liverpool.ac.uk/
- Email: servicedesk@liverpool.ac.uk
- Telephone: 44567 (internal)
- Telephone: +44 (0) 151 794 4567 (external)

Or you can visit the Service Desks:

- CSD building on Brownlow Hill (building 224, F7) open Monday-Friday 8:30am to 5pm
- Sydney Jones Library (building 443, F3) open Monday-Friday, 9am to 5pm
- Harold Cohen Library (building 431, D8) open Monday-Friday, 9am to 5pm

8. Information Security Incident Response (Roles and Responsibilities)

Source/Reporter

It is important that anyone who reports a security incident provides as much relevant information as possible. Anticipated sources for reporting Information Security Incidents are expected to come from, but not limited to:

- Staff/student(s) of the University
- Faculty Security Manager(s)
- Approved Authorities/External Parties (e.g. JANET)
- Member(s) of the Public

CSD Security Incident Response Team (SIRT)

The team consists of the Computing Services senior management team (CSD SMT) along with relevant technical teams. This group is authorised to take decisions on behalf of the University to ensure that core IT services and day to day activities are resumed and that any risks to the University and its information assets are managed and mitigated accordingly.

The Director of Computing Services will, on advice and guidance from the Security Incident Response Team (SIRT) and technical teams, ensure that appropriate steps are taken to address any security weaknesses which have been identified.

Risk Level and Criticality

All security incidents are categorised by the actual and potential risk impacts on day to day activities of the University. For additional information on severity determination and how these are categorised please refer to the University Risk Management Policy.

Risk, Definition and Response Times

Risk Level & Definitions		Priority Level	Initial Response Times	RACI Model	Communication Requirement
Very High/High	Security incident affecting critical systems or confidential/strictly confidential information assets. High impact on revenue and/or reputation of University.	1/2	1 hour	SIRT Team Technical Teams Asset Owners/Data Controllers	Case update will be sent a **minimum of every 2 hours.**

Medium/High	Security incident affecting critical systems or confidential/strictly confidential information assets. Significant impact on revenue or reputation of University.	2/3	8 Hours 1 Day	SIRT Team Technical Teams Asset Owners/Data Controllers	Case update sent to appropriate parties on a **daily** basis during critical phase.
Low/Medium	Possible security incident, non-critical systems or non-sensitive information assets. No potential or actual damage to the University's finances or reputation.	3/4/5	48 Hours 72 Hours+	SIRT Team Technical Teams Asset Owners/Data Controllers	Case update sent to appropriate parties on a **weekly** basis.

Definitions

Risk Level & Definitions – this is determined by the level of threat (likelihood/impact) against the University information assets and will be dealt with in accordance to level of risks, day to day operations and the criticality of the information assets which are under threat.

Initial Response Times – Agreed SLAs/OLAs and criticality of response times based on Severity/Criticality/Risk Level to information assets. These SLAs and OLAs are owned by the CSD Customer Services Manager. These response times are defined as part of the SIRT "working hours". For more information on these working hours please refer to the Customer Services Manager.

RACI – Responsible, Accountable, Consulted, Informed (these are the relevant stakeholders that must be communicated within one of the capacities above) - undertaking the work or managing the process of the work e.g. Faculty Managers, Technical teams and asset owners.

Communication Requirements – These are the standard communication requirements as underlined by SLAs to ensure that relevant stakeholders are notified of the work being undertaken and any other impending problems to information assets/services.

Triage Meeting

Specific information security events and incidents will determine different types of responses and resources required. In the event of University wide or pandemic situations the SIRT may require input and communication with various University stakeholders and asset owners' e.g. Immediate Response Team (IRT) and the Business Recovery Group (BRG) to ensure a relevant strategy is agreed to ensure timely mitigation of risks to the University. Please refer to the Incident Management and Business Continuity Policy for more information.

Technical Team(s)

The technical teams will be the University Subject Matter Experts (SMEs) who provide guidance and advice, or undertake the actions required to investigate information security events/incidents. Once events and incidents have been raised via the CSD Service Desk or a member of the SIRT, specific teams may be required to undertake specific works and actions to ensure risk mitigation.

Investigation/Root Cause Analysis (Type 1)

These are determined as non-user specific investigations (in which the activity of an individual is not being investigated) and may be associated with University wide or CSD input to investigate events and problems. The technical teams will undertake appropriate root cause analysis and actions to minimise the risk to University core business operations.

Mitigation/Corrective Action

Mitigating actions will be undertaken to minimise risks or disruption of the University's services. These activities will normally be undertaken by relevant CSD staff to prevent incidents re-occurring. Alternatively they may include a workaround that ensures University business operations are continued. Please refer to the Information Security Review Policy for more information.

9. User Investigations (Type 2)

If an initial analysis indicates involvement, suspicious or malicious behaviour by an individual, a member of the SIRT will advise the relevant line manager accordingly. It is then the responsibility of the relevant manager (or his/her equivalent) to request a formal user investigation. For more information on user Investigations, please refer to the Security Investigations Policy.

10. External Parties

In extenuating circumstances, the Computing Services Department may contact third parties to help resolve information security incidents. For example, if the incident involves the JANET network then the JANET Computer Security Incident Response Team (CSIRT) may be contacted. This process will only be activated by the Security Incident Response Team.

CSD may need to provide information or require input from approved authorities or other areas of the University as part of the wider incident response and continuity plans. For all major security incidents, CSD SMT will communicate with the relevant internal/external stakeholders accordingly.

11. Information Security Incident Response Process

12. Legal Obligations and University Policies

This policy is aimed at all staff/student(s) of the University who have a responsibility for the usage, management and ownership of University assets. This policy is part of the University Information Security Management System (ISMS) and should be read in conjunction with the Information Security Policy and its sub policies and relevant UK legislation(s). Further relevant policies and legislation(s) are listed in Appendix A.

13. Compliance and Monitoring

All staff/student(s) of the University are directly responsible and liable for the information they handle.

Members of staff are bound to abide by the University IT regulations by the terms of their employment. Students are bound to abide by the University IT Regulations when registering as a student member of the University.

Authorised staff members of the University may monitor the use and management of information assets to ensure effective use and to detect unauthorised use of information assets.

Appendix A – University ISMS Reference

- Regulations for the Use of IT Facilities at the University of Liverpool
- JANET Acceptable Use policy
- Information Security Policy
- Workspace and IT Equipment Security Policy
- Information Asset Classification Policy
- Information Security Review Policy
- IT Procurement and Third Party Security Policy
- IT Asset Disposal Policy
- Security Investigation Policy
- Procurement Policy
- Data Protection Policy
- Freedom of Information Policy
- Copyright Policy
- Card Payment Policy
- Records Management Policy
- Records Retention Policy
- Risk Management Policy
- Student/HR Disciplinary Procedures

Relevant legislation includes:

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Data Retention Investigatory Powers Act 2014
- Counter Terrorism and Security Act 2015 (Prevent)
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002

Relevant Regulation includes:

- PCI-DSS (Payment Card Industry Data Security Standards)