Sheffield Hallam University

Managing Information Security Incidents Policy

Issuing Authority:	Leon Etherington, Acting Chief Information Officer, Information Systems and Technology
Signed:	
Date Effective:	March 2016
Review date:	February 2018
Version:	2016.2

Managing Information Security Incidents Policy

Objective

To outline procedures to identify and resolve Information Security Incidents quickly, and to resume normal service as soon as possible.

Scope

This policy applies to all University staff, students, data processors, partners, suppliers and contractors and other authorised users when working with University IT systems and infrastructure.

Definition

An Information Security Incident is an actual or suspected event that presents a threat to the confidentiality, integrity or availability, of information, or that puts at risk the security of the IT infrastructure and systems.

Policy Requirements

1. All members of the University, and all visitors and third parties who are granted access to the University's IT system and information systems shall comply with the **IT Security Policies, Procedures and Related Guidance** (formally the Electronic Information Security Framework - EISF) and all ***Supporting Policies*** to minimise the likelihood of security incidents.
2. Individuals shall not attempt to look for potential security risks without authorisation from the Acting Chief Information Officer of IS&T. All Information Security Incidents, actual or perceived, shall be reported as soon as possible to ITHelp.

ITHelp extension: 3333 or email: ithelp@shu.ac.uk

3. On receipt of an Information Security Incident report, the IT Security Officer shall record the incident, and arrange to secure any evidence and equipment that would be required to investigate the incident.
4. If written authorisation from the Director of IS&T is received, the IT Security Officer shall then arrange to investigate the equipment secured and collate detailed evidence.
5. All investigations into Information Security Incidents shall be conducted, and records of the investigation kept, according to the best practice guidelines; **HEIDS/J-LIS Inappropriate Use of Investigation Process**.
6. An investigation into an Information Security Incident shall be halted immediately at any stage if material of a criminal nature is found. Advice should then be sought with a view to handing over the investigation to the police or other law enforcement agencies.
7. All evidence secured during an investigation into an Information Security Incident shall be given a unique identifier, sealed, and retained in a secure area.
8. Information about reported Information Security Incidents, and the results of any investigations, shall not be published or divulged, except on a need-to-know basis.
9. All investigations of Information Security Incidents shall be reviewed by the IT Security Forum. Major Information Security Incidents or significant risks to Information Security brought to light by an investigation shall be reported by the IT Security Forum to the appropriate University committee.

10. If investigation of an Information Security Incident involves the monitoring of the activities of one or more members of the University, this shall be authorised and conducted in accordance with the ***University Monitoring Policy***.

11. Any breach of security, or of the ***Regulations for the Use of IT Facilities*** shall be the subject of investigation and possible further action. The ***Disciplinary Procedure*** for staff and ***Disciplinary Regulations for Students*** shall be followed in such cases. Suspected breaches of the law may be reported to the police.

All requests from the police and law enforcement agencies for assistance with enquiries into computer misuse or other criminal activities are to be immediately directed to the University Secretary and Registrar and the IT Security Officer informed of the request and any action taken.