Appendix E

University of Central Lancashire
IT Security Incident Handling Guide

This document is prepared and managed by LIS as part of the Information Management Guide on behalf of the University and contains guidance for Users of IT facilities following a definite or suspected breach of Information Security controls as detailed in the University IT Security Policy, or breach of the rules detailed in the IT Facilities Rules document.

All IT based systems across the University are covered by this document.

Change History:

	Date	Status	Responsible
Original	July 1999	Issued	G Ashton
Revised	January 2005	Issued	G Ashton
Revised	December 2005	Issued	G Ashton
Revised	July 2010	Issued	G Ashton
Next revision due	July 2011		

Introduction

This guide should be read in conjunction with the *IT Security Policy* and the *IT Facilities Rules*. Both of these documents can be found at www.uclan.ac.uk/aup

This guide seeks to raise User awareness of IT security incidents in very general terms. It also stresses that Users should not attempt to investigate such incidents themselves, but all relevant information should be promptly reported so that investigators can carry out such work according to current best practice.

To report an IT Security incident, call LIS Customer Support on extension 5355.

A security incident can occur at any time, and when a report is received, an investigation will usually begin immediately to determine the details and mitigate any consequences.

Depending on the nature of the incident, the investigation may be directed towards finding ways of avoiding a repetition. However, an investigation may uncover evidence leading to a User having action taken against them by the University under its rules, regulations and policies.

- Where student misconduct is suspected, the Academic Standards and Quality Unit may be involved in the investigation.

- Where staff misconduct is suspected, the Human Resources service will be involved in the investigation.

- Where an incident is suspected to involve a *Data Protection breach* i.e. loss or theft of personal data, investigators will inform the university's *Data Protection Officer* as a matter of course.

- Where an incident is believed to involve an actionable crime, it will be escalated to law enforcement agencies via SDS.

LIS is authorised to access, modify, remove access to or delete any data items or services on University networks to facilitate investigations or remedial actions.

The nature of IT Security incidents requires that investigators have in depth technical knowledge of the systems involved, and expertise will need to be drawn in where appropriate. Where the incident occurs within, or originates from, a subsidiary system managed by a University department, that department must investigate the event (in conjunction with LIS as appropriate) and provide a report to LIS on the event and the conclusions, including a summary of any remedial action taken.

Due to the broad range of possible events and causes, this guide can only be general.

What is an IT Security Incident?

Where university information is concerned, an IT Security incident can be defined as any event or set of circumstances threatening its confidentiality, its integrity or its availability.

Confidentiality – The information is restricted to those rightfully needing to access and process it as part of their jobs.

Integrity – There is confidence in the quality and reliability of the information i.e. it is correct, up to date and complete as opposed to inaccurate, out of date, corrupted or missing.

Availability – The information can be rightfully accessed when needed. Access is not prevented by interference from any person or system.

Incidents can also more broadly involve suspicions of

- inappropriate use of IT systems
- hacking (unauthorised access/technical break-in)
- virus infections or other malicious software
- computer based crime (for example, child pornography or activity related to terrorism)

The above list is not exhaustive.

Discovery of an IT Security Incident

An incident or suspected incident can be discovered in many ways:-

- A User suspecting their account has been used by someone else
- Unauthorised access to specific IT facilities by a third party
- Breach of confidentiality, suspected malpractice or misuse of university information
- Signs that unauthorised modification of information has taken place
- Possible misuse of workstation out of hours, or suspected tampering
- Possible attempt to break into or infiltrate a computer system
- Suspicious approaches or persuasion to disclose passwords or information
- Other suspicious circumstances or behaviour
- Loss/theft of a memory stick or portable computing device (including PDAs and smartphones) containing university information
- Misaddressed email containing confidential information
- Possible illegal material accessed or stored on system i.e. child pornography or terrorism related information
- Computer virus infection
- Reports from Users, anonymous sources, or external complainants
- Unauthorised changes to IT systems
- Lapsed physical security

Signs of suspicious activity on a computer system may be noticed by its administrators. Such signs must always be properly investigated, and never ignored.

How to Report an IT Security Incident - Guidance for Users

To report an incident or suspicious circumstances, Users should without delay contact **LIS Customer Support** on extension **5355**.

LIS Customer Support will instruct Users on action to take immediately with regard to the matter reported.

All reports will be treated in the strictest confidence, and knowledge of incidents and investigations is restricted on a need-to-know basis.

Handling of computer workstations and other equipment

Some types of incident may directly involve particular workstations or other equipment. When such an incident is first reported, the general advice given to Users is to ensure the equipment is left untouched and preserved in its current state before investigators arrive. This preservation is very important for computer forensics, as computer based evidence is fragile and could be damaged by actions that are normally considered harmless, such as starting or closing applications..

This means Users present at the time

- should not touch the keyboard or the mouse
- should not press the reset button
- should not press the on/off switch
- should not disconnect any leads
- should not themselves attempt to shut down the machine in any way

Users should always follow the advice given at this stage.

Initial Response

On receiving a report, LIS Customer Support will immediately alert IT Security staff, who will make direct contact with the Users to progress.

Investigation

Matters reported will always be handled confidentially and investigations will be conducted according to current best practice.

An individual's right to privacy will always be respected. Intrusive examinations of User activity, such as email or Internet usage, will only be performed if absolutely necessary and justified in the circumstances. Investigators must therefore obtain management authorisation before actions which could intrude on privacy are carried out.

Depending on the nature of the incident, the investigation may identify one or more causes or contributing factors

- problems with working practices or procedures
- University rules, regulations and policies not being followed
- technical weaknesses of IT systems which could lead to security breaches
- attempted or successful technical attacks on IT systems
- inappropriate use of IT systems
- suspected criminal acts involving IT systems