GISP14. Incident reporting and handling

Date:	5 October 2017
Version:	2.0
Authors:	Raymond Scott
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
1.1	5/10/17	Reviewed and updated
2.0	20/10/17	Approved by ISSC

Policy

Security Control	Procedures and structures for reporting and handling security incidents and suspected security weaknesses.
Objective	• To ensure that security incidents are reported and handled according to defined procedures and policies. • To ensure a consistent response to incidents commensurate with the security risk posed and in compliance with legislation. • To ensure and encourage the reporting of suspected security weaknesses. • To ensure the monitoring of potential security threats. • Where it is necessary to collect evidence against a person or organisation, it shall be collected and presented to conform to the relevant rules of evidence.
Policy	14.1. All security incidents and breaches of this Security Policy should be reported immediately following defined and publicised procedures on the ITCS website. 14.2. All security incidents and breaches will be treated seriously and handled according to defined procedures. Where illegal activity is detected, this will be reported to the appropriate authorities. 14.3. Where it is necessary to collect evidence against a person or organisation, it shall be collected and presented to conform to the relevant rules of evidence. Expert guidance may be required.
Responsibility	• ITCS is responsible for defining and publicising procedures for reporting and handling information security incidents. • ITCS is responsible for investigating information security incidents and taking appropriate action. In cases where illegal activity, or activity in breach of University regulations, has taken place, initial evidence will be collected and forwarded to the appropriate authority for them to consider further actions. • ITCS is responsible for monitoring and reviewing potential security threats.

	• ITCS is responsible for reviewing security breaches and ensuring that appropriate steps are taken to reduce the likelihood of further occurrence.
Incident management	Security and misuse incidents should be reported and handled according to the procedures described below. Logs of actions taken, including times and dates should be kept. Where IT security mechanisms are discovered to have been seriously breached, the manager responsible for the systems/area should be immediately informed and they should take immediate action to mitigate.
Audit and accountability	The Assistant Director Strategy, Policy and Compliance should annually review incident reporting and handling procedures, consulting with involved parties regarding any proposed changes. The Principal Investigator for any incident should keep records of any investigations and subsequent actions. IT Support Managers and IT service managers should take account of any incidents that have occurred when performing the annual review of the IT Services Risk Log.
Implementation	**Suspected security weaknesses and threats** • Suspected security weaknesses should be reported to the IT Service Desk who will pass details on to the appropriate Service Head. • All security breaches, threats and weaknesses will be reviewed by the IT Management Team which will have mechanisms in place to learn from those incidents. **Security incidents** For the purpose of reporting/handling security incidents and computer misuse, three broad categories of incident are defined here: • **System security incident** - Where activity has been detected which has led to, or could lead to, unauthorised access to UEA IT systems, or disruption to services and systems. • **Inappropriate use incident** - Where activity has been reported or detected which is believed to contravene the University's Conditions of Computer Use • **Data and compliance breach incident** - Where sensitive data has been lost or stolen. For example breach of copyright, theft of IP, etc. Procedures for reporting and handling the above types of incident are detailed below: **System security incidents** • Any incident detected on centrally managed services/systems, should be reported to the IT Service Desk who will alert the appropriate IT Service Head who will take remedial action. • Incidents detected on Faculty managed services/systems should be reported to the IT Service Desk who will alert the appropriate IT Support Manager who will take remedial action. • The IT Service Desk will take suitable measures to ensure that users are informed if a service is affected.

	• A record of each incident should be kept by the Service Head or IT Support Manager. These are reviewed monthly by the IT Management Team. Records should include incident details, date, time and actions taken. • Where illegal activity has been detected which requires reporting to the Police, all details should be forwarded to Strategy, Policy and Compliance team, who will coordinate evidence gathering and reporting to the Police, liaising with HRD, SSS, senior management and security as appropriate. Assuming that the equipment poses no wider threat then no further action should be taken. If there are concerns that the equipment may pose a threat to University services, then it should be disconnected from the network. **Inappropriate use incidents** • Inappropriate use by staff - Incidents should be reported to HRD via the appropriate Human Resources Manager or senior management. Appropriate action will then be taken and the Strategy, Policy and Compliance team and other University officers informed/advised as appropriate. • Inappropriate use by students – Incidents should be reported to the appropriate Head of School or senior management. The Head of School will then take appropriate action, consulting with SSS and SPC as appropriate. • Receipt of inappropriate email - Unless the sender of the email is a member of the University, these should be reported to the IT Service Desk. There is guidance available on ITCS web pages on what should/should not be reported; see URL below: https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/it-regulations-and-policies/user-guidelines/reporting-emails-with-inappropriate-content If the sender of the email is a member of the University, the incident should be reported as per inappropriate use detailed above. • For incidents reported to the IT Service Desk, the Service Desk will if appropriate refer details to the Strategy, Policy and Compliance team for investigation and follow-up. • Where a serious matter is reported to the Strategy, Policy and Compliance team, they will consult with HRD, SSS or senior management depending on whether staff or students are involved. If initial investigation points to potential illegal activity, Strategy, Policy and Compliance team will liaise with HRD, SSS, senior management and security as appropriate to ensure the matter is reported to the Police. • Where inappropriate use involves members of the University, strictest confidentiality will be maintained when dealing with these incidents. **Data and compliance breach incidents** • All data and compliance breaches should be reported to the Strategy, Policy and Compliance team, who will take appropriate action which may need to involve external agencies.