ISC10D026

Report Control Information

Title:	General Information Security Policy
Date:	28 January 2011
Version:	v3.08
Reference:	ICT/GISP/DRAFT/3.08
Authors:	Steve Mosley
Quality Assurance:	ISSC

Revision	Date	Revision Description
V3.0	13/12/05	Final version as approved by the Information Strategy and Services Committee (ISSC) on 2nd of December 2005.
V3.01	2/2/07	Minor change to GISP15 under 'Incident Response' in order to take account of staff changes – Incidents now reported to the ICT Policy Officer in ITCS.
V3.02	6/2/07	GISP5 Use of passwords – location of best practice guidelines changed.
V3.03	7/3/07	Active links to other documents (e.g. Security Manual) inserted.
V3.04	16/7/07	Link errors corrected in GISP4
V3.05	3/8/07	Link errors corrected in GISP10
V3.06	9/6/08	GISP25 – Changed to link to new Self-Registered Equipment Terms and Conditions
V3.07	23/6/08	GISP3 – Links to Security Manual corrected
V3.08	TBC	Changes to GISP following review of security policies and implementation in 2010, and recommendations from external consultants.

Please note: Although active links to the Security Manual have been inserted where this is referenced, some security controls within the Security Manual may not yet have been developed and approved.

General Information Security Policy

Contents

Introduction

Aims and objectives

The General Information Security Policy has been developed to address security concerns regarding all electronic information within the University. The three main objectives of the Policy are:

- Confidentiality: To ensure that information assets and services are only accessed by authorised parties.
- Integrity: To ensure that information assets can only be modified by authorised parties and only in authorised ways. The definition of 'modified' includes, created, written to, changed, have its status changed and deleted.
- Availability: To ensure that information assets and services are accessible to authorised parties at appropriate times.

During implementation of this Policy all services and assets will be assessed to ensure that the above objectives are considered during the design, creation, development, deployment, modification, maintenance and disposal of assets and services.

Organisation of the Policy

This document details the security policies applying to the University's network, telecommunication systems, IT and computing systems and the information stored on these. All members of the University and visitors using the University's IT and computing facilities and associated telecommunication systems are expected to be aware of and comply with those policies which apply to their area of use. It is the responsibility of heads of Faculties, Schools and Units to ensure their staff and students are aware of and comply with these policies.

The policies are organised in four sections:

- **Policies applying to all users** – policies that apply to all users of the University's network, IT and computing systems and telecommunication systems.
- **Policies specific to staff** – policies in addition to those applicable to all, which are specific to University staff.
- **Policies specific to students** – policies in addition to those applicable to all, which are specific to students of the University.
- **Policies applying to visitors** – policies which are specific to visitors using the University's network, IT and computing systems and telecommunication systems e.g. conference delegates, consultants employed by the University and academic visitors to Schools.

Policy review and monitoring

Information Services is responsible for the review and monitoring of this Policy which will be checked on a regular basis in order to ensure compliance with legislation, and that recognised best practice is followed.

Consultation with appropriate consultative bodies and stakeholders within the University will be undertaken before any changes to the Policy are proposed. Proposed changes will be submitted to the Information Strategy and Services Committee (or relevant successor body) for approval and an annual report reviewing the Policy will be submitted to this committee.

Policies applying to all users

GISP1. Risk assessment and risk management

Security Control	University IT services and computing and telecommunication systems will be subject to regular risk assessment and management.
Objective	• To ensure that the security of the University's IT services and computing and telecommunication systems is reviewed on a regular basis. • To determine risks, their impact and the managed response required to remove the risk or reduce its impact.
Policy	1.1 The security of all University IT services and computing and telecommunication systems will be reviewed at least annually and a risk log produced for each service/system (Security Manual SM1.1).
Responsibility	• Information Services are responsible for all centrally managed systems and services. • Schools/Units are responsible for their own systems.
Incident Response	New risks identified should have their impact promptly assessed and a managed response determined.

GISP2. Conditions of Computer Use

Security Control	The Conditions of Computer Use define the policies and guidelines that all individuals must comply with when using University computing and network facilities.
Objective	• To encourage responsible behaviour and good practice by individuals when using computing facilities and network and telecommunication systems. • To ensure that the University is compliant with the requirements of the Joint Academic Network (JANET) Acceptable Use Policy. • To ensure the University is compliant with all government legislation in relation to information technology, computing and telecommunications.
Policy	2.1 All users of University computing and network facilities must be aware of and abide by the Conditions of Computer Use which are available on the University Intranet at http://www.uea.ac.uk/is/itregs/usepols 2.2 Breaches of the Conditions of Computer Use by a member of the University will be treated as a disciplinary matter.
Responsibility	• All those who use University computing facilities have a personal responsibility to be aware of and comply with the requirements of the Conditions of Computer Use. • Departments should ensure that the Conditions of Computer Use are brought to the attention of all users that they are responsible for.
Incident Response	Any suspected breaches of the Conditions of Computer Use should be reported to either the Information Service's ICT Policy Manager, or in their absence the Director of Information Services . If appropriate they will initiate any investigation and will inform and engage with the Human Resources Division, Dean of Students Office and/or head of department as appropriate. All information received will be treated in a confidential manner, only involving other individuals where strictly necessary to any investigation. A form has been setup on the University's website for reporting misuse: http://www.uea.ac.uk/is/itregs/misuse.

GISP3. Physical and environmental security

Security Control	Physical access to computer and telecommunication systems will be restricted to authorised users only.
Objective	• To ensure that only those authorised to do so can physically access computer and telecommunication systems. • To prevent theft and unauthorised tampering with computer resources.
Policy	3.1 All computer systems must be located in an environment which is secure against theft and complies with University building security recommendations. 3.2 Computers in student IT areas should be secured in accordance with policies and procedures detailed in the Security Manual SM3.1 Physical security for IT systems (ref SM3.1.5 to SM3.1.7). 3.3 Computer servers and telecommunications equipment should be housed in especially secure areas to which physical access is controlled with only authorised users being allowed access - see Security Manual SM3.1 Physical security for IT systems (ref SM3.1.8 to 3.1.10). Such areas should have appropriate heating and air conditioning so as to maintain operability of the systems and integrity and availability of the data stored on them.
Responsibility	• For centrally managed services, physical access to computer servers will be the responsibility of Information Services. • Departments are responsible for the physical security of their servers located in their building. Where department servers are located in Information Service's computer suites, their physical security will be the responsibility of Information Services. • For computers located in staff offices it is the responsibility of the occupier to ensure that their office is locked when no one is there.
Incident Response	Breaches of physical security will be investigated by the manager responsible for security of the area concerned. In the case of break-ins/theft these should be reported to the University Security Office who will liaise with the Police.

GISP4. Identification, authentication and authorisation

Security Control	Individual usernames and passwords will be used to authenticate access by authorised users to all University computer systems and IT services.
Objective	• To ensure that only authorised users can access University computer systems and IT services. • To ensure that individuals accessing computer systems and services can be identified. • To control access to restricted computer systems and IT services.
Policy	4.1 All individuals using University computer systems or IT services must be authorised to do so. 4.2 All authorised users will be assigned a unique University username and password in accordance with defined policies and procedures (GISP5.1 and Security Manual SM5.1). 4.3 Access to sensitive data such as personnel data will be authorised by designated data owners following defined policies and procedures.
Responsibility	• The Registrar and Planning Office are responsible for defining who should have access to University IT and computing services. • Information Services will provide and implement authentication mechanisms to control access, following defined policies and procedures (see 4.2) • Data owners are responsible for authorising individual's access to sensitive data (see 4.3). • Individuals must not attempt to access systems or services for which they are not authorised (see also GISP2, Conditions of Computer Use).
Incident Response	All suspected breaches of authentication mechanisms should be reported immediately to Information Services via the IT Helpdesk who will initiate investigation and appropriate action, including liaising with data owners/administrators where necessary.

GISP5. Use of passwords

Security Control	Access to all University computer systems is controlled by use of individual usernames and passwords.
Objective	To prevent unauthorised access to computer systems.
Policy	5.1 All access to University computer systems will be controlled by use of a unique username and password limiting access to each user of the system. 5.2 All default passwords assigned to individuals will be secure and follow defined rules (Security Manual SM5.1). 5.3 System administrator passwords will be restricted to specific authorised personnel following defined policies and procedures (Security Manual SM5.3).
Responsibility	• Individual users are responsible for keeping their password secure and not divulging it to anyone else. • If individuals change their password, they should ensure that it is secure and conforms to University approved best practice as published on the Information Services web-site. • Those responsible for assigning and communicating passwords to individuals must follow rules and procedures as detailed in the following documents: o Security Manual SM5.1 'Password Assignment' o Security Procedure SP1 'Communicating passwords to users'. • Passwords should not be disclosed to anyone other than the individual concerned..
Incident Response	• If a user's password (and hence their IT account) is found to have been compromised, it will be changed immediately by Information Services to a new secure one and the user informed. • Where an individual suspects that an unauthorised person is using another's password to access University computer systems, they should report the incident immediately to the IT Helpdesk

GISP6. Use of email

Security Control	University Email service for secure email correspondence.
Objective	To provide a secure and confidential email service for both staff and students.
Policy	6.1 The University will provide a secure email service for all members of the University. 6.2 An individual's email will be secure against unauthorised access by other individuals via the use of individual usernames and passwords (see GISP4 and GISP5). 6.3 Anti-virus mechanisms will be implemented on the University's email gateways to help prevent virus infected email attachments reaching a user's inbox (see also GISP10, 'Protection against malicious software'). 6.4 Anti-Spam mechanisms will be implemented on the University's email gateways to aid in reducing the volume of unsolicited email reaching a user's inbox. 6.5 The University reserves the right to access an individual's University email account in the course of investigating a breach of University regulations, where illegal activity is suspected, or in the case of unexpected absence by staff, to ensure University business is not delayed or hindered (see Conditions of Computer Use). 6.6 If confidential data is being transmitted via email, senders should ensure that this is sent in an encrypted format, or as a password protected attachment with the password conveyed to the recipient by means other than email (e.g. by telephone).
Responsibility	• Information Services is responsible for providing a secure email service for staff and students. • Individuals using provided email services must comply with the Conditions of Computer Use.
Incident Response	Any breaches of email security should be immediately reported to the IT Helpdesk.

GISP7. Network access control

Security Control	All equipment connected to the University network must be registered.
Objective	To ensure that only equipment which has been registered can connect to the network.
Policy	7.1 All equipment connected to the University network must be registered following the approved registration procedures (Security Manual SM7.1). 7.2 Any equipment detected on the network which has not been registered will be immediately disconnected. 7.3 Changes in ownership of connected equipment should be notified to Information Services following approved change notification procedures.
Responsibility	• Information Services will provide mechanisms for registering equipment requiring connection to the University network (see 7.1 and 7.3). • Individuals should not attempt to connect any equipment which has not been registered to the University network.
Incident Response	Any non-registered equipment detected on the network should be reported immediately to the IT Helpdesk.

GISP8. System access controls

Security Control	All connections to University systems will be secured against unauthorised access.
Objective	• To ensure that only authorised users can connect to University computer systems. • To ensure that connections to University computer systems use secure protocols.
Policy	8.1 All University computer systems will be protected against unauthorised access as detailed in GISP4 (Identification, Authentication and Authorisation) and GISP5 (Use of Passwords). 8.2 All University computer systems will be protected against unauthorised connections from external computers (i.e. those not registered on the University's network) by a University firewall (Security Manual SM8.1). 8.3 Authorised connection to University computer systems from external computers will be enabled by rules on the firewall, which will be approved and configured according to defined policies and procedures (Security Manual SM8.1). 8.4 Where possible all connections to University computer systems will use secure protocols which ensure that information, including usernames and passwords, are passed between systems in an encrypted format (Security Manual SM8.2).
Responsibility	• Information Services is responsible for maintaining the University firewall and for authorising any requests for external access to University systems (see 8.2 and 8.3). • Information Services will provide secure channels for connecting to computer systems (see 8.4). They will also ensure suitable software is provided on the University's Standard Staff and Student Desktops to enable users to securely connect to services, including login access, file transfer and email. • Users should not attempt to circumvent system access control mechanisms.
Incident Response	Any suspected breaches of the University's system access controls should be reported immediately to the IT Helpdesk.

GISP9. Change management

Security Control	All University IT and computing facilities/services to be maintained in a secure state irrespective of any changes to infrastructure or business processes.
Objective	To ensure that security matters are considered as an integral part of any change process where IT and computing facilities, or information processing is involved.
Policy	9.1 Security issues must be seriously considered in any process or project where the IT and computing infrastructure may be changed, or the manner in which information is processed is likely to change. Where a project is particularly reliant on IT and computing facilities/services, security should be addressed under a specific heading within the project plan. 9.2 Where IT and computing facilities/services are subject to change compliance with relevant legislation should also be reviewed (see GISP17)
Responsibility	• Information Services will advise on best practice. • Project managers are responsible for ensuring that security matters are seriously considered in projects involving IT and computing facilities, or information processing.
Incident Response	If IT facilities/services are discovered to be insecure, this should be reported to Information Services, who will investigate and address matters with relevant project managers and stakeholders.

GISP10. Protection against malicious software

Security Control	All computer systems must be protected against the threat of malicious software.
Objective	To prevent infection of all University computer systems, including servers, desktop systems and laptop/notebook computers, by malicious software such as viruses, trojans, worms, key loggers etc.
Policy	10.1 All computer operating systems must have up to date security patches installed, and have in place mechanisms for automatic patching of the operating system (Security Manual SM10.1). 10.2 All computer systems must have University approved software installed (where such exists) to protect against malicious software such as viruses, Trojans, worms, key loggers etc. The software and associated data files should be installed and configured following defined policies and procedures (Security Manual SM10.1).
Responsibility	• Information Services will monitor malicious software threats and will provide central services for automatic updating of supported operating systems and approved software used to protect against such. • IT support staff are responsible for ensuring deployed systems have up to date operating system patches and anti-malware software installed and correctly configured (see 10.1 and 10.2).
Incident Response	• Any computer system found to be infected with malicious software will be disconnected from the network until the software has bee removed. • Any computer system discovered to be not up to date in respect of either operating system patches, or anti-malware software will be immediately referred to the IT support staff responsible for that system and these will in turn remedy the situation as soon as possible (see 10.2).

GISP11. Information classification

Security Control	All University information will be assigned to an Information Class
Objective	• To ensure that all information has an assigned Information Class. • To ensure that each Information Class has agreed standards for data storage, handling, transmission and disposal.
Policy	11.1 All information stored on University computer systems will be assigned to an Information Class which will determine how the data is to be stored, handled, transmitted and disposed of (Security Manual SM11.1).
Responsibility	• Information Services will publish and maintain a University approved Information Classification scheme giving guidelines on best practice for storing, handling, transmitting and disposing of data. • Data Managers are responsible for determining a dataset's Information Class using the above scheme, and for ensuring the data is stored and handled in accordance with the guidelines for that Class.
Incident Response	Where data is discovered not to be stored or handled in accordance with its Information Class, this should be reported to the appropriate Data Manager.

GISP12. Secure areas

Security Control	Access to secure areas must be strictly controlled and monitored.
Objective	To ensure that access to computer and telecommunications systems in secure areas/buildings is strictly controlled and monitored with only authorised individuals having access.
Policy	12.1 All secure areas must comply with University building security recommendations. 12.2 Documented authorisation and authentication procedures and mechanisms must be implemented for every secure area to ensure that only authorised individuals can access the area (Security Manual SM12.1). 12.3 Where sensitive data is stored in secure areas, network access to that data must be carefully controlled and monitored following documented procedures (Security manual SM12.1). 12.4 Each secure area must have a designated individual responsible for day to day security of that area.
Responsibility	• University Security is responsible for overall building security on campus. • The manager of a secure area within a building is responsible for the security of that area.
Incident Response	• Breaches of building security should be reported immediately to University Security. • For secure areas within buildings, breaches of security should be reported to the manager for the area in question.

GISP13. Business continuity

Security Control	A Disaster Recovery Plan will be in place to protect the University's critical business processes from major failure of IT and computing services or disaster.
Objective	To ensure that in the case of a major failure or disaster affecting University IT services or telecommunications, a plan for restoring essential services exists.
Policy	13.1 A Disaster Recovery Plan which supports the University's Business Continuity Plan will exist for all IT and computing services and telecommunication systems. 13.2 The Disaster Recovery Plan will be reviewed annually and disaster recovery plans for any new systems will be tested before those systems go live.
Responsibility	Information Services is responsible for maintaining and reviewing a Disaster Recovery Plan.
Incident Response	In the event of a major catastrophe affecting IT and computing services or telecommunication systems the Disaster Recovery Plan will be consulted and appropriate action taken.

GISP14. Incident reporting and handling

Security Control	Procedures and structures for reporting and handling security incidents.
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.
Policy	14.1 All security incidents and breaches of this Security Policy should be reported immediately following defined and publicised procedures - system administrators refer to Security Manual SM14.1 and end-users to procedures publicised on the IT and Computing Service web-site. 14.2 All security incidents/breaches will be treated seriously and handled according to defined procedures (Security Manual SM14.1). Where illegal activity is detected this will be reported to the appropriate authorities.
Responsibility	Information Services is responsible for defining and publicising procedures for reporting and handling information security incidents. Information Services 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 University authority for them to consider further actions.
Incident Response	All reported incidents will dealt with according to defined procedures (see 14.2).

GISP15. Monitoring and use

Security Control	Monitoring of network traffic to identify security threats.
Objective	To ensure that network traffic is monitored in order to detect activity in breach of this Information Security Policy and/or the Conditions of Computer Use
Policy	15.1 Regular monitoring of use of the University Data Network and the Internet will be undertaken for the purpose of maintenance, fault-finding purposes, prevention of denial of service attacks and enforcement of this Information Security Policy and the Conditions of Computer Use. See also section 5.3 of the Conditions of Computer Use. 15.2 The University reserves the right to undertake more detailed monitoring if there are reasonable grounds to believe that a user has committed a criminal offence or is otherwise in breach of the Conditions of Computer Use. 15.3 Where activity is detected which poses a risk to other users of the network, or which could seriously reduce network performance, the University reserves the right to disconnect offending machines/users from the network until the matter has been investigated. 15.4 Various activities on the network, including websites visited, may be routinely logged for diagnostic and evidential purposes.
Responsibility	Information Services is responsible for monitoring use of the University network and for reporting any activity in breach of this Policy and/or the Conditions of Computer Use to the appropriate agency within the University.
Incident Response	Incidents detected by network monitoring will be reported to the ICT Policy Manager in Information Services who will take appropriate remedial action and/or report to the appropriate agency within the University for further action. Incidents to be reported to the police will be done so via University Security.

GISP16. Health and safety

Security Control	All IT and computing systems and services provided by the University will be compliant with the University's Health and Safety Policy.
Objective	To ensure use of computer systems is compliant with the University's Statement of Safety Policy, and in doing so ensure compliance with all legislation in this area.
Policy	16.1 All computer systems deployed must be compliant with the University's Statement of Safety Policy – see http://www.uea.ac.uk/menu/admin/uss/safepolr.pdf .
Responsibility	• The University's Safety Service is responsible for publishing and maintaining a University Health and Safety Policy. • Heads of departments must ensure that any computer systems belonging to their department comply with the University's Health and Safety Policy.
Incident Response	Breaches of the University's Health and Safety Policy should be reported to the University's Safety Service.

GISP17. Legal and regulatory compliance

Security Control	All IT and computing systems will comply with current legislation
Objective	• To ensure that all University IT and computing systems comply with UK government legislation. • To ensure that use of the University network is in accordance with regulations of the Joint Academic Network (JANET).
Policy	17.1 All University IT and computing systems and information services hosted on these must be compliant with current UK government legislation. 17.2 All use of the University network and its connections to the internet must be compliant with JANET regulations.
Responsibility	• Information Services is responsible for making users, system administrators and data owners aware of legislation with which they must comply. • Individual users are responsible for ensuring their own actions and any systems they are responsible for comply with current legislation (see also GISP2, Conditions of Computer Use).
Incident Response	Where it is suspected that a computer system, service or activity does not comply with legislation, the matter should be reported to the owner of the system or service involved.

GISP18. Security standards, guidelines and best practice

Security Control	Use of network and IT and computing systems should follow security standards
Objective	To ensure that users are aware of and comply with University security standards, guidelines and best practice.
Policy	18.1 All users of the University's network and IT and computing systems should be aware of and act in accordance with this security policy and University published guidelines and best practices.
Responsibility	• Information Services is responsible for monitoring guidelines and best practice as developed for universities by external agencies such as JISC and UCISA, and for making users aware of best practices that should be followed within the University. • Heads of departments and line managers are responsible for ensuring their staff follow IT and Computing service guidelines.
Incident Response	Where it is discovered that best practice is not being followed, this should be reported to the appropriate line manager, or in the case of a centrally provided service to the IT Helpdesk.

Policies specific to staff

GISP19. Accountability and accessibility of University owned assets

Security Control	Ensuring University IT and computing assets are known, and access to these assets is managed.
Objective	• To ensure that the University is fully aware of all IT and information assets which it owns and there is a registered 'owner' responsible for each asset. • To ensure that migration and disposal of assets is managed according to defined procedures ensuring the University is compliant with financial regulations and relevant legislation. For information assets see also GISP11 Information classification.
Policy	19.1 Inventories of all University owned IT and information assets will be maintained which includes an 'owner' for that asset who is responsible for its day to day security. Information assets should be classified according to the Information classification policies (GISP11). 19.2 Disposal of assets at the end of their useful life within the University will be in accordance with University financial regulations and external legislation governing such. Disposal of computing hardware must be done in compliance with the University's policies regarding such (see Desktop Computer Procurement and Deployment Policy section 4)
Responsibility	• It is the responsibility of each Faculty or service unit to maintain up to date inventories of its IT and computing assets and to make this available to appropriate authorities within the University on request.
Incident Response	Where asset information has been compromised, the 'owner' of that asset should be notified.

GISP20. System specific

Security Control	Security controls specific to staff workstations
Objective	To ensure that staff workstations, including desktop and laptop/notebook systems, are secure against malware threats and unauthorised access.
Policy	20.1 Staff workstations must be secured against unauthorised access (see Security Manual SM20.1). Also see GISP4 Identification, authentication and authorisation, GISP5 Use of passwords. 20.2 Staff workstations must have up to date operating system patches installed and protection against malicious software – see GISP10.1 and GISP10.2.
Responsibility	• IT support staff responsible for deploying and supporting staff workstations should ensure systems are installed in accordance with procedures for securing workstations. • Information Services will provide and maintain guidelines and procedures for securing workstations. • Workstation users should not attempt to circumvent the security controls on workstations
Incident Response	Where a workstation is found to be insecure, this should be reported to the relevant IT support staff for them to rectify.

GISP21. Encryption use and key material handling

Security Control	Control of encryption use by staff
Objective	• To ensure that encryption use for University data is in accordance with defined policies and procedures. • To ensure the ability to undertake University work is not adversely affected by the use of encryption.
Policy	21.1 Use of encryption to protect University data should be in accordance with the University's policies on information classification - see GSP12 Information Classification. 21.2 Where encryption is used to protect sensitive data, or in the case of electronic communications, confirm the identity of the sender, the encryption method used should follow University defined procedures (Security Manual SM21.1) 21.3 When encryption is used, details of the encryption method and keys should be securely stored and accessible to the user's line manager.
Responsibility	• Information Services is responsible for determining and publishing procedures and guidelines for using encryption. • It is an individual's responsibility to ensure that encryption is only used where justified and in accordance with this Policy and the University's information classification policies. • Note, in the course of any criminal investigation involving encrypted data, an individual may be required to give police access to encryption keys used, or to prove that the keys are no longer in their possession. If University owned data is involved, the administrator for that data, or the project manager would normally be responsible for providing access to encryption keys used.
Incident Response	Where encryption procedures and processes have been compromised the incident should be reported to the administrator for the data concerned, or to their line manager.

GISP22. Corporate responsibilities and conduct

Security Control	Staff responsibilities/conduct conducive to good security
Objective	To ensure that staff conduct is not detrimental to good IT and information security.
Policy	22.1 All staff irrespective of their role, should ensure that their conduct whilst using IT and computer systems is conducive to good security and is in accordance with University security guidelines, this Policy and the Conditions of Computer Use (see also GSP3 Conditions of Computer Use). 22.2 All staff handling information should do so in accordance with Information classification policies (GISP11).
Responsibility	• Individual staff should be aware of University guidelines and policies relating to security and their use of IT and computer systems. • Line managers for staff should make their staff aware of security guidelines and policies and where necessary take action to ensure the conduct of their staff is commensurate with good security. • Information Services will publish security guidelines and policies on the intranet.
Incident Response	Where the conduct of a member of staff is suspected to be detrimental to good security, the matter should be reported to the line manager for that member of staff for them to take appropriate action.

GISP23. Personnel security

Security Control	Controls' ensuring that appropriate consideration is given to information security roles and responsibilities of staff.
Objective	To ensure that staff using information processing facilities within the University understand their responsibilities in regard to information security, and the risk of human error, theft, fraud or other mis-use is minimised.
Policy	23.1 Where appropriate to the post, staff job descriptions should contain details of information security roles and responsibilities. 23.2 Pre-employment checks (e.g. taking up of references) should take account of the information security requirements of a post and ensure that the candidate is suitable in this respect. 23.3 All staff with information processing duties will receive appropriate guidelines and training in regard to information security. 23.4 On termination of employment, procedures should be followed to ensure that all access rights to University information or information processing facilities are removed.
Responsibility	• The Human Resources Division (HRD) is responsible for ensuring that procedures and guidelines for the drafting of job descriptions and appointment of staff take adequate account of information security roles and responsibilities. • Line managers are responsible for providing staff with the appropriate guidelines and training in regard to their information security roles and responsibilities. • Staff should be aware of their information security roles and responsibilities and carry out their work in accordance with these.
Incident Response	If it is suspected that the above controls/policies have not been followed, the matter should be reported to HRD.

Policies specific to students

GISP24. Liability of students' own systems and content

Security Control	Controls to ensure that student owned systems do not compromise security, or introduce liabilities for the University.
Objective	To ensure that student owned computer systems or personal data owned by students do not compromise security or give rise to any claims against the University.
Policy	24.1 All student owned systems must first be registered before connection to the University network is permitted. (see GSP8 Network access control) 24.2 All student owned systems connected to the University's network, or student owned data stored on University servers must be in accordance with University regulations, the Conditions of Computer Use (see GISP2) and Self-registered Equipment - Terms and Conditions (see GISP25). 24.3 The University accepts no responsibility for either the safety or security of student owned systems.
Responsibility	• Information Services is responsible for providing a secure network and method of connection for student owned equipment. A secure email system and central filestore will also be provided for the use of students in conducting their studies. • Students are responsible for ensuring their personal computer systems are safe, secure and legal, and for ensuring their password(s) for accessing University services are secure (see also GISP5).
Incident Response	Incidents should be reported to the IT Helpdesk. If a student owned system, or data is found to be in contravention of this policy, access to the network, or data may be denied, depending on the level of risk to the University. Further action will be taken where appropriate.

GISP25. Residences network terms and conditions

Security Control	Terms and conditions of connection to the University's residences network.
Objective	• To ensure all computer systems connected to the University's residences network are done so in accordance with relevant legislation and regulations. • To ensure all computer systems connected to the University's residences network pose a minimal security risk to services and other users on the network.
Policy	25.1 All use of network connections in student residences must be in accordance with the Self-Registered Equipment Terms and Conditions at http://www.uea.ac.uk/is/itregs/selfregtc 25.2 The University reserves the right to disconnect any network access point within residences, and take appropriate further action, where its use has contravened the above terms and conditions.
Responsibility	• Information Services is responsible for maintaining and publicising the Residences Network Terms and Conditions and monitoring use of the network. • Individual residents are responsible for the use of network connections within their rooms, irrespective of whether or not they own equipment that is connected to the network point.
Incident Response	Where it is discovered that a network connection is being used in contravention of the Self-Registered Equipment Terms and Conditions, that network point will be disconnected from the network and further action taken.

GISP26. Identification, authentication and authorisation of student systems

Security Control	Access to the University network and services from student owned systems will be identifiable and appropriately authenticated and authorised.
Objective	To ensure only registered student owned systems can access the University network and services that they are authorised for.
Policy	26.1 All student owned systems connected to the University network must be registered. See also GSP8 Network Access Control. 26.2 All access via student owned systems to University IT and computing services will be authorised and authenticated. See also GSP5 Identification, Authentication and Authorisation relating to all users.
Responsibility	• Information Services will ensure that control mechanisms are in place to ensure appropriate identification, authentication and authorisation of student owned systems. • Students should not attempt to circumvent control mechanisms, or attempt to use a non-registered computer on the University network.
Incident Response	Where a student owned system is found to be circumventing the above controls, this should be reported to the IT Helpdesk who will arrange for immediate action to be taken.

GISP27. Encryption use and personal liability

Security Control	Control of encryption use by students
Objective	To ensure encryption use by students is in accordance with University policies and not detrimental to the University.
Policy	27.1 Students should only encrypt University data if the project they are working on, or University service they are using, requires such. 27.2 Where encryption is used, the encryption method used should follow University defined procedures (Security Manual SM21.1) 27.3 When encryption is used, details of the encryption method and keys should be securely stored and be accessible to the manager/supervisor of the project they are working on.
Responsibility	• Information Services is responsible for determining and publishing procedures and guidelines for using encryption. • It is an individual's responsibility to ensure that encryption of University data is only used where justified and in accordance with this Policy and the University's information classification policies. • Note, in the course of any criminal investigation involving encrypted data, an individual may be required to give police access to encryption keys used, or to prove that the keys are no longer in their possession. If University owned data is involved, the administrator for that data, or the project manager would normally be responsible for providing access to encryption keys used.
Incident Response	Where encryption procedures and processes have been compromised the incident should be reported to the administrator for the data concerned, or to the project manager.

GISP28. Student responsibilities and conduct

Security Control	Controls to ensure students use the University network and services in a responsible fashion.
Objective	To ensure students act in a responsible fashion when using the University network and services and in such a manner as to not negatively impact on the security of University IT and computing systems.
Policy	28.1 All students using University IT and computing systems/services must act in a responsible manner in accordance with this security Policy and with the University Conditions of Computer Use (see GISP2).
Responsibility	• Information Services is responsible for making students aware of regulations and guidelines governing IT and computing system/service use. • Individual students are responsible for ensuring their conduct is in accordance with this security policy, University regulations and relevant external legislation they have been made aware of.
Incident Response	Where the conduct of a student is in contravention of the above policy, appropriate action will be taken and where necessary the matter will be reported to the appropriate student disciplinary body.

Policies specific to visitors

Visitors to the University include, visiting members of faculty, external consultants or contractors doing work on behalf of the University, attendees at University organised conferences or training courses, and members of the public who by special arrangement have been authorised to use University IT facilities and services.

GISP29. Liability of own systems and content brought to University

Security Control	Controls to ensure that visitor owned systems do not compromise security, or introduce liabilities for the University.
Objective	To ensure that visitor owned computer systems connected to the University network do not compromise security or give rise to any claims against the University.
Policy	29.1 All visitor owned systems must first be registered before connection to the University network is permitted. (see GSP8 Network access control) 29.2 All visitor owned systems connected to the University's network, or visitor owned data temporarily stored on University servers must be in accordance with University regulations and the Conditions of Computer Use (see GISP2). Where visitors are connecting equipment to the network, they must abide by the Self-Registered Equipment Terms and Conditions (see GISP25). 29.3 The University accepts no responsibility for either the safety or security of visitor owned systems.
Responsibility	• Information Services is responsible for providing a secure network and method of connection for visitor owned equipment. • Visitors are responsible for ensuring their personal computer systems are safe, secure and legal.
Incident Response	Incidents should be reported to the IT Helpdesk. If a visitor owned system, or data stored on University filestore is found to be in contravention of this policy, access to the network, or data may be denied, depending on the level of risk to the University. Further action will be taken where appropriate.

GISP30. Identification, authentication and authorisation of visitors' systems

Security Control	Individual usernames and passwords will be used to authenticate access by visitors to any University computer systems or IT services they have been authorised to use.
Objective	To ensure that visitor access to University IT and computing systems and services is identified, authorised and authenticated as for members of the University
Policy	30.1 Any visitors who have been authorised for access to a University IT and computing system or service, will be subject to the same controls as for members of the University – see GISP4 Identification authentication and authorisation for all users.
Responsibility	As for GISP4.
Incident Response	As for GISP4

GISP31. Key messages ("Thou shalt not")

Security Control	Making visitors aware of the key prohibited actions.
Objective	To ensure that visitors are aware of key policies that they must not contravene.
Policy	31.1 Visitors must not intentionally contravene the University Conditions of Computer Use in any way – see link below: http://www.uea.ac.uk/is/itregs/usepols 31.2 If residing in University residences, visitors must not contravene the Self-Registered Equipment Terms and Conditions at http://www.uea.ac.uk/is/itregs/selfregtc 31.3 No visitors IT equipment should be used on the University network without having been registered for such. 31.4 No visitor's computer should be connected to the University network without up to date anti-virus software being installed and operational. 31.5 Visitors should not attempt to run any software whose use is prohibited by the University, either on their own system connected to the University network, or on University owned systems. See references to prohibited software in the Conditions of Computer Use (31.1) and the Residences Network Terms and Conditions (31.2). 31.6 Visitors must not disclose to anyone else passwords which have been allocated to them for the purpose of authorised access to University IT and computer systems. 31.7 Visitors must not take any action to circumvent any University security control that is in place.
Responsibility	Visitors are responsible for ensuring that they are aware of the above policies and abiding by them.
Incident Response	Any visitor found to be in contravention of these policies will immediately have their access rights removed. Where a member of the University discovers that a visitor is in breach of these policies, they should report the incident immediately to the IT Helpdesk.

GISP32. Encryption use and key handling

Security Control	Control of encryption use by visitors.
Objective	• To ensure that any encryption applied by visitors to University data is in accordance with defined policies and procedures. • To ensure the ability to undertake University work is not adversely affected by the use of encryption.
Policy	32.1 A visitor should only encrypt University data where authorised to do so and in accordance with the University's information classification policies (see GISP11). 32.2 Where encryption is used in University work, the policies and procedures as for University staff should be followed – see GISP 21, Encryption use and key material handling for staff.
Responsibility	• It is the responsibility of the project manager for the work where the visiting consultant is employed to ensure that encryption use by the consultant is in accordance with this Policy and University information classification policies. • It is the visiting consultant's responsibility to ensure they follow University policies and guidelines in relation to encryption. • Note, in the course of any criminal investigation involving encrypted data, an individual may be required to give police access to encryption keys used, or to prove that the keys are no longer in their possession. If University owned data is involved, the administrator for that data, or the project manager would normally be responsible for providing access to encryption keys used.
Incident Response	Where encryption procedures and processes have been compromised the incident should be reported to the project manager.

GISP33. Visitor responsibilities and conduct

Security Control	Controls to ensure visitors use the University network and services in a responsible fashion.
Objective	To ensure visitors act in a responsible fashion when using the University network and services, and in such a manner as to not negatively impact on the security of University IT and computing systems.
Policy	33.1 All visitors using University IT and computing systems/services must act in a responsible manner in accordance with this security Policy and with the University Conditions of Computer Use (see GISP2)
Responsibility	• Information Services is responsible for making visitors aware of regulations and guidelines governing IT and computing systems/services use. • Individual visitors are responsible for ensuring their conduct is in accordance with this security Policy, University regulations and relevant external legislation they have been made aware of.
Incident Response	Where the conduct of a visitor is in contravention of the above policy, appropriate action will be taken.