Report Control Information

Title:	General Information Security Policy
Date:	24/02/2020
Version:	V5.2
Document Owner	Matt Roach
Quality Assurance:	Information Strategy and Services Committee (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 Management' 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	20/1/11	Approved by ISSC 14th February 2011. Changes to GISP following review of security policies and implementation in 2010, and recommendations from external consultants.
V3.10	18/9/12	Fully revised, rewritten and restructured. Earlier references to section numbers have not been preserved.
V3.11	2/10/12	Updated following ISD review.
V3.12	25/10/12	Updated following community review.
V4.0	8/11/12	Updated following ISSC review. Approved by ISSC
V4.1	7/2/13	Added policy on information system timeout to GISP24
V4.2	28/5/13	Revised procedure for communicating passwords in GISP5
V4.3	4/10/17	Updated to accommodate requirements of PCI DSS and reflect changes to University department structures and roles
V5.0	20/10/17	Approved by ISSC
V5.1	16/10/18	Updated after external audit

V5.1	24/02/20	Document reviewed during December 2019 and January 2020; no changes identified. Review status confirmed by ITCS Leadership Team and Chief Operating Officer. 'Author' changed to 'Document Owner' and changed from Raymond Scott to Matt Roach

General Information Security Policy

Introduction

Aims and objectives

The General Information Security Policy has been developed to address security concerns regarding all electronic information within the University. Information Security is considered to comprise the following three aspects:

- **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.

As part of the implementation of this Policy with respect to all assets and services, an assessment is to be carried out to ensure that the above objectives are considered during the design, creation, development, deployment, modification, maintenance and disposal of assets and services.

The General Information Security Policy is a collection of statements addressing the aims and aspirations for information security at the University. Where an implemented solution or service is unable to achieve the standard set in these policies, a risk assessment should be conducted to confirm that the risk is acceptable and if so the non-compliance should be recorded as a risk against that service. GISP1 describes policy on risk assessment and management.

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.

Governance and implementation

The Information Strategy and Services Committee (ISSC) has oversight of the University's information security policies. ITCS will work with individuals and departments to deliver solutions compliant with these policies. It will also provide advice, guidance and training to the University community to raise awareness, develop understanding and good practices and minimise risk. Where resources allow, ITCS will work with the internal auditor and engage third party services to provide assurance of compliance with these policies.

Policy review and monitoring

ITCS 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. The information Security Policy will be reviewed at least annually and updated when the environment changes.

Information security key points

The set of General Information Security Policies contains detail on the security controls and policy statements to which the University aspires. Within each policy, there is additional guidance on how that policy should be implemented. Listed below are keys points to be drawn from this set of policies.

Information Risk Management:

- Information security is more than an IT issue. It is a strategic risk management issue
- Identify key information assets and apply an appropriate level of protection to them. For instance, backup data to ensure its availability
- Actively consider risks associated with the security of the information that you manage or handle
- Be proactive in managing information security. It is not enough just to respond to incidents
- Security controls and information security policies should be commensurate with the level of risk that can be tolerated. This means we need to decide our appetite for risk
- Changes in technology such as cloud computing or mobile devices can shift the balance of risk. New technologies should be subject to an information security risk assessment before introduction

Incident Management:

- There must be established and tested plans and processes to restore service and information assets after failure or loss
- Plans should be in place to manage the impact of and recovery from an information security incident

Advice & Guidance:

- Users should be informed of acceptable and secure use of University systems
- Users should have training on information security, and regularly made aware of risks
- New users should be briefed on information security as part of their induction
- Threats are not only technical, but can also involve social engineering – e.g. tricking a user to click on a malicious link, or pretending to be someone else to reset their password
- All users should respond to and act on notices from ITCS on perceived security threats

Managing User Privileges:

- Accounts should be issued and deleted according to set and agreed processes
- Users should have user account privileges according to their role
- Minimise the number of user accounts with elevated privileges, as these pose a higher risk

Secure Configuration:

- All systems including personally-owned systems should be kept up to date with the latest security patches and protected against malware
- Maintain hardware and software inventories of University assets to inform the need for updates

Monitoring:

- Centrally managed systems should be monitored continuously for unusual activity
- Security controls should be regularly reviewed and tested to ensure they are being followed and are effective. Non-compliance may be down to a lack of training or point to a need for policy revision
- Users should be aware that their activity may be monitored, especially those handling sensitive information

Network Security:

- The University data network should be protected against external and internal attack
- Security should be regularly tested by undertaking penetration tests simulating the behaviour of a malicious attack and to discover vulnerabilities

Mobile devices:

- Information stored on a mobile device (e.g. mobile phone, laptop, USB stick, CD) is particularly at risk of loss or theft
- Mobile devices should be used securely and configured to prevent unauthorised access
- Take special care with handling the security of information when in transit (e.g. attached to an email, stored on a mobile device, shared via a collaboration tool)

Further information

https://www.gov.uk/government/policies/cyber-security

Policies

GISP1. Risk assessment and risk management

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	University information 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 information 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 risks associated with all University information services will be reviewed at least annually and a risk log produced.
Responsibility	Service owners are responsible for ensuring that risk assessment and management is undertaken
Incident management	New risks identified should have their impact promptly assessed and a managed response determined.
Audit and accountability	Annually updated risk logs for all information services within UEA will be reviewed by the IT Forum (ITF) and IT Support Managers before being submitted to the Information Strategy and Services Committee (ISSC). ITCS will co-ordinate this activity.
Implementation	• ITCS will produce a Risk Log Template for use with centrally managed services and by Faculties. • ITCS will identify a list of all services they operate and using the Risk Log Template will record any significant security risks threatening these services and mitigating action to be taken. • Faculties will identify a list of all services they operate and using the Risk Log Template will record any significant security risks threatening these services and mitigating action to be taken.

	• Those responsible for a service should review the Risk Log for that service at least annually and whenever there is a significant change to the service, or whenever a serious security incident affects the service. • Risk Logs for all services will be reviewed annually by ITCS with the IT Forum and IT Support Managers and thereafter submitted for consideration by ISSC. This activity to be co-ordinated by ITCS.

GISP2. Conditions of Computer Use

Date:	5 October 2017
Version:	2.1
Document Owner:	Matt Roach
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
2.1	18/01/18	Review by external auditor

Policy

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 website at https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/it-regulations-and-policies/usage-policies 2.2. Breaches of the Conditions of Computer Use by a member of the University will be treated as a disciplinary matter. 2.3. A nominated person is responsible for preparing guidelines to ensure that all staff and students are aware of the key aspects of computer misuse legislation (or its equivalent), in so far as these requirements impact on their duties.
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. • ITCS are responsible for reviewing the Conditions of Computer Use on an annual basis. • ITCS will ensure that all staff and students are reminded of their responsibilities under the Conditions of Computer Use on an annual basis.
Incident Management	Any suspected breaches of the Conditions of Computer Use should be reported to the IT Service Desk or, if of a sensitive nature, reported to Data Protection Officer, or in their absence the Director of IT. If appropriate, they will initiate any investigation and will inform and engage with the Human Resources Division, Student Support Services 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 is available on the University's website for reporting misuse: https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/it-regulations-and-policies/report-computer-misuse

GISP3. Physical and environmental security

Date:	5 October 2017
Version:	2.1
Document Owner:	Matt Roach
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
2.1	18/01/18	Review by external auditor

Policy

Security Control	Physical access to computer and telecommunication systems proportionate to the sensitivity of the data held on those systems will be managed to restrict access 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 information assets • 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 Screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons. 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.
Responsibility	• For centrally managed services, physical access to computer servers will be the responsibility of ITCS. • Departments are responsible for the physical security of their servers located in their building. Where department servers are located in ITCS's computer suites, their physical security will be the responsibility of ITCS. • 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 Management	Breaches of physical security will be investigated by the manager responsible for security of the area concerned. The investigating manager is responsible for assessing the impact of any unauthorised data access and this should be reported to the IT Service Desk or, if of a sensitive nature, reported to Data Protection Officer, or in their absence the Director of IT. In the case of break-ins/theft these should be reported to the University Security Office who will liaise with the Police.
Audit and accountability	IT Support Managers and relevant managers in ITCS should audit physical security of systems in their charge on a regular basis (at least annually), taking remedial action as appropriate. Outstanding issues and deviation from these controls should be recorded in the annual Security Policies Issues Log which is collated by ITCS and submitted to ISSC for review.
Implementation	**IT areas** In open access areas such as student IT areas: • Systems should be secured to the desk to guard against theft. • Systems should be configured to automatically logout after 30 minutes of non-use. • Students should be warned (e.g. by notices) that they should not leave an unattended system logged in. **Staff offices** Key owners/occupants of staff offices are responsible for ensuring overall room security, but should in respect of IT systems in their offices adhere to the following practices: • When absent from the office and no one else is in it, ensure that the office is locked and secure. • When absent from the office, ensure that mobile devices and laptop computers are locked away wherever practical. • Blinds should be drawn on office windows overnight to guard against external viewing of IT equipment. • Confidentiality/privacy should be maintained on systems by automatically locking the system when unattended after 15 minutes. This is particularly important in shared offices where confidential information may be viewed on the screen. • All PCs should be logged out and powered off at the end of the working day. • All sensitive information should be secured from unauthorised accessed at the end of the working day, a clear desk policy should be considered. **Servers and telecommunications equipment** • Servers and telecommunications equipment should be secured in special purpose rooms which are secured against unauthorised access and theft by University approved door access control mechanisms. Such access control mechanisms should record who has been authorised to access the area and who has entered an area at a particular point in time. Procedures should be in place to ensure that when a person ceases employment with the University, or their role changes to one without access rights to the area, their access rights are changed accordingly on the system.

	• Where it is necessary to locate telecommunications equipment in multiple locations across campus (e.g. network switches), the equipment should be locked away to safe guard against unauthorised access and tampering. Key holders should be recorded and strictly controlled. • Server backups should be stored in a fire safe to which access is restricted to authorised individuals and for which records are kept of transferrals to/from the fire safe. Where disaster recovery policies/procedures require so, backups should be housed away from the server area, or off-site.

GISP4. Identification, authentication and authorisation

Date:	5 October 2017
Version:	2.1
Document Owner:	Matt Roach
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
2.1	16/10/18	Review by external auditor

Policy

Security Control	Individual usernames and passwords will be used to authenticate access by users to authorised 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). 4.3. Access to sensitive data such as personnel data will be authorised by designated service owners following defined policies and procedures. 4.4. Access controls shall be maintained at appropriate levels for all systems by on-going proactive management and any changes of access permissions must be authorised by the manager of the system or application. A record of access permissions granted must be maintained. 4.5. Inactive user accounts are either removed or disabled within 90 days of leaving 4.6. Terminated user accounts will be either removed or disabled immediately. 4.7. Where other authentication methods are used (e.g. physical or logical security tokens or smartcards), they must be assigned to an individual account and not shared between accounts. Controls must be in place to ensure that only the intended account can use the mechanism to gain access.

	4.8. For systems within scope of PCI DSS, Multi factor authentication (MFA) will be implemented for all individual non-console administrative access and all remote access to system components in the CDE by users, administrators and third parties (such as support and maintenance or vendors). MFA is required for: a. All non-console access into the CDE for personnel with administrative access. b. All remote network access into the CDE (user, administrator and third parties) originating from outside the network.
Responsibility	• The Registrar and Planning Office are responsible for defining who is a member of the University. • The Information Strategy and Services Committee is responsible for deciding which IT services are made available to members of the University. • ITCS will provide and implement authentication mechanisms to control access, following defined policies and procedures. • Service owners are responsible for authorising individual's access to sensitive data. • Individuals must not attempt to access systems or services for which they are not authorised (see also GISP2 and Conditions of Computer Use).
Incident Management	All suspected breaches of authentication mechanisms should be reported immediately to ITCS via the IT Service Desk who will initiate investigation and appropriate action, including liaising with data owners/administrators where necessary.
Implementation	Inactive accounts must be disabled or removed within 90 days. • The identity management system will be configured to automatically disable users once their course end date, employment contract end date or visitor access end dates have been reached. Terminated users should be disabled or removed immediately. • Terminated users will have their account disabled manually within the Identity Management system or the source data system (HR or SITS) updated with the appropriate end date for the user.

GISP5. Use of passwords

Date:	5 October 2017
Version:	3.1
Document Owner:	Matt Roach
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
1.1	28/5/13	Procedure for communicating passwords reviewed
2.0	11/6/13	Approved by ISSC
2.1	5/10/17	Reviewed and updated
3.0	20/10/17	Approved by ISSC
3.1	16/01/2018	Review by External Auditor

Policy

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. 5.3. System administrator passwords will be restricted to specific authorised personnel following defined policies and procedures. 5.4. Passwords must be changed every 90 days for accounts being used to access system components within scope for PCI DSS. 5.5. Access to operating system commands and application system functions is to be restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored.
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 ITCS website. • Those responsible for assigning and communicating passwords to individuals must follow rules and procedures as detailed below in 'Communicating passwords to users'.

	• Passwords should not be disclosed to anyone other than the individual concerned.
Incident Management	• If a user's password (and hence their IT account) is found to have been compromised, it will be changed immediately by ITCS 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 Service Desk. • Where system administrator security is discovered to have been breached, this should be reported immediately to the support staff responsible for security of the system. If it is discovered that the security controls described here have not been adhered to, the matter should be referred to senior management responsible for the system(s) involved.
Audit and accountability	All IT support staff will on request by ITCS confirm that all computer systems under their control are using the University's defined rules/policies for passwords. For computer systems whose authentication is against the Active Directory, the defined rules/policies will be automatically applied to both local and domain user accounts. A risk assessment should be undertaken for any IT system which is not capable of supporting the password policy, this risk assessment should be reported to ISSC. System owners who have computer systems in their care, will on a regular basis review administrator password security arrangements and check that the procedures described here are being followed. In particular they will check that written records of administrator passwords and those with authorised access are accurate, are stored securely and are not available to unauthorised personnel.

Implementation	**All Users**
	• All user accounts on University computer systems, irrespective of the type of computer system or account, must be assigned passwords which meet the following minimum requirements.
	  • User account passwords must be at least eight characters in length
	  • Passwords for administrator accounts and user accounts with administrative rights must be at least fifteen characters in length
	  • Not contain the user's account name
	  • Contain characters from at least three of the following four categories:
	  1. English upper case characters (A through Z)
	  2. English lower case characters (a through z)
	  3. Base 10 digits (0 through 9)
	  4. Non-alphanumeric characters (e.g. !, $, #, %)
	• Passwords should expire 365 days after the date they were last changed or created.

	• Authentication mechanisms should force the user to change from their default assigned password to a new one at first login to the system and after a password reset. • Authentication mechanisms should be configured to allow a maximum of 5 attempts to enter a password, after which the user's account should be automatically locked against access for a period of 30 minutes. After 30 minutes access to the account should automatically be re-enabled. • All mechanisms for assigning or changing passwords should be set to automatically apply the rules described above and in addition ensure that the previous five passwords from the password history cannot be used. • Passwords previously used either for accounts at UEA or outside of UEA should not be used. • Passwords must be stored on computer systems as a non-reversible cryptographic hash using the strongest hash available for the operating system. For Windows based systems a NoLMHash policy should be applied to avoid storing passwords as Lan Manager hashes, instead using the stronger NT/Unicode hash. Password safes (such as KeePass) may be used for password transmission and storage. Passwords should not be transmitted in plain text format for any purpose. Access to stored cryptographic hashes must be restricted to as few people as is possible whilst allowing normal operational and administration procedures to be undertaken. • Defined procedures must be followed when communicating default passwords to computer users – see 'Communicating passwords to users' below. • Additional defined policies and procedures are to be followed for the storage and handling of system administrator passwords. • Defined procedures must be followed if a user suspects that their password has been compromised. **Server administrators (including domain administrator and root accounts)** • Wherever possible, support staff whose role requires administrator privileges on a server should have those privileges applied to their normal UEA IT account by including them as a member of the appropriate administrator's group within Active Directory. If their role changes and system administrator privileges are no longer required, they should be promptly removed from the administrator's group[1]. Where actual system administrator passwords have to be disclosed to support staff, the following guidance should be adhered to.

[1] When staff leave UEA, their IT account is automatically deleted and hence their membership of the administrator group.

	• All system administrator account passwords (including domain administrator and root accounts) should adhere to the password assignment rules as defined above and except for additional requirements as applied to administrator account passwords, follow best practice as published at http://www.uea.ac.uk/is/itregs/userguide. Wherever possible, the password should be randomly generated and should be unique to the computer/service. • System administrator passwords should be disclosed to as few staff as is practically possible in order to maintain operation of a service. Procedures should be in place to ensure that disclosure of passwords is only authorised by the manager of the system(s) and to ensure that those receiving the password acknowledge receipt and their responsibility to keep the password secure and not disclose it to others. • Additional security is required for system administrators of critical systems within the scope of PCI DSS and those processing personal data. Tiered accounts should be used to separate system administration and development environments from desktop environments. The accounts used to access systems within scope of PCI DSS must have their passwords/pass phrases changed at least every 90 days. • System administrator passwords must be changed on a regular basis, at least twice per year and whenever a member of staff who has known the password ceases to be employed by the University, or moves to a different post whose duties do not require system administrator access to the system(s) concerned. • A written record of the current system administrator password along with a list of those to whom it has been disclosed, should be stored in a safe and secure place, access to which is restricted to the manager responsible for the system(s) and a nominated deputy. All previous records of system administrator passwords should be destroyed. **Desktop local administrator accounts** • Where possible, desktop local administrator accounts should be disabled. If this is not possible, they should only be enabled for the duration of the requirement. • IT support staff, whose role requires that they have local administrator access to desktop systems in their care, should have those privileges applied to their normal UEA IT account by including them as a member of the appropriate administrator's group within Active Directory. If their role changes and system administrator privileges are no longer required, they should be promptly removed from the administrator's group. • Separate administrator groups should be set up for each department following Active Directory Organisational Units (OUs) and IT support staff computers should be excluded so that they do not automatically have administrator privileges on their own computer.

	• Desktop local administrator account passwords should only be used where privileges as described above are insufficient to resolve a problem, and direct access via the local administrator account is essential. In such cases, the following guidance should be followed. Procedures should be in place to ensure that the password is only distributed to authorised IT support staff and a log is maintained of those who have access to the password. • Staff (including IT support staff) requiring local administrator privileges on their office computer will have to request this from the IT support manager for their department and give justification for this. Local administrator privileges will only be granted for a finite period of time. • The local administrator account password on a desktop system should adhere to the same password assignment rules as applied to servers and defined for server administrators. • The local administrator password should only be disclosed to those IT support staff who have responsibility for supporting and maintaining the system and only when the usual administrator privileges granted to them are not sufficient to fix a problem. • Local administrator passwords should be disclosed to as few staff as is practically possible in order to maintain operation of a service. Procedures should be in place to ensure that disclosure of passwords is only authorised by the manager of the system(s) and to ensure that those receiving the password acknowledge receipt and their responsibility to keep the password secure and not disclose it to others. • Local administrator passwords must be changed on a regular basis, at least twice per year and whenever a member of staff who has known the password ceases to be employed by the University, or moves to a different post whose duties do not require system administrator access to the system(s) concerned. • A written record of the current local administrator password along with a list of those to whom it has been disclosed, should be stored in a safe and secure place, access to which is restricted to the manager responsible for the system(s) and a nominated deputy. All previous records of system administrator passwords should be destroyed. **Communicating Passwords to Users** These basic procedures should be followed when communicating passwords to users, either to new users, or when dealing with incidents where a password change has been required and this needs to be communicated to the user.

	• Only those staff authorised to do so should communicate passwords to users. For ITCS managed IT accounts, such as the UEA IT account allocated to all staff and students, only IT Service Desk staff should inform users of their password following separate additional detailed procedures documented in Service Desk operational documents[2]. • Other staff authorised to inform users of passwords, such as IT support staff allocating passwords for accessing local departmental IT resources where authentication is not controlled by centrally managed Active Directory processes, or course administrators who have been allocated a batch of visitor IT accounts by ITCS for distribution to attendees, should follow the procedures below: o Wherever possible the user should be informed of the password by face to face contact. Before informing the user of the password, their identity should be checked[3]. o Where face to face contact is not possible, the user's password should be communicated to them over the telephone after asking them to confirm their full name, their staff or student number, and at least one other piece of information that has previously been collected as part of the authorisation process such as date of birth or home postcode. o The password should be communicated to no other person other than the user, and the user should be reminded that they must keep the password secure and must not under any circumstances disclose it to any other person. o Wherever possible the resource/facility being accessed should be configured to force a change of password when the user first accesses the resource/facility[4] and after every occasion that the password is reset. If this is not possible/practical, they should be instructed to change the password at the first opportunity. o Passwords should never be sent via email or any other digital communication mechanism to recipients.

[2] Service Desk operational documents are stored on the ITCS intranet with access restricted to the Service Desk and other authorised ITCS staff.

[3] Where the user has been allocated a campus card they can be checked against the photo on the card.

[4] Enforcing a change of password when first accessing the facility will depend on the type of facility being accessed.

GISP6. Use of email

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	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) and that appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed and that the recipients are authorised to receive it. 6.7. Acceptable use of the University email services as defined in the Conditions of Computer Use.

Responsibility	• ITCS 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. • Individuals using provided email services should ensure that all emails are addressed correctly.
Incident Management	Any breaches of email security should be immediately reported to the IT Service Desk.
Implementation	• All users should follow the guidance on email best practice available from the web page https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/it-regulations-and-policies/user-guidelines/email-guidelines • Emails sent to parties outside the University should include the standard disclaimer notice https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/it-regulations-and-policies/user-guidelines/email-disclaimer-notice • Where appropriate, a confidentiality notice should be added to emails https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/it-regulations-and-policies/user-guidelines/email-confidentiality-notice

GISP7. Onsite access control

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	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. To ensure unregistered devices have limited access to the University network containing self-registration and password reset services.
Policy	7.1. All equipment connected to the University network must be registered following the approved registration procedures 7.2. Any equipment detected as active on the network which has not been properly registered will be disconnected. 7.3. Devices that have been detected as not used on the network within the previous 6 months will be unregistered. 7.4. Changes in ownership of connected equipment should be notified to ITCS following approved change notification procedures.
Responsibility	• ITCS will provide mechanisms for registering equipment requiring connection to the University network. • Individuals should not attempt to connect any equipment which is excluded under the Conditions of Computer Use.
Incident Management	Any equipment detected on the network or access to the network which contravenes the conditions of computer use should be reported immediately to the IT Service Desk.
Audit and Accountability	ITCS will maintain a DNS/DHCP record for all equipment registered on the University network and will ensure this is up to date at all times and secure against unauthorised access.
Implementation	**University-managed equipment** • Only nominated IT Support staff may register University owned equipment on the network.

	• A web based form will be provided for this purpose which will enable registration of equipment on the network. • Registration details will be collected and processed according to defined procedures. • IT support staff should ensure that equipment being registered is virus free, has University approved anti-virus software installed (see GISP10), and poses no risk to security of the network or other equipment connected to it at the time of registration. **Personally-managed computers connected via Ethernet port in University residences** • Student and visitor owned computers must be registered by the owner raising a ticket with the IT Service Desk. Registration details will be collected and processed according to defined procedures. • Access to authorised University services will be mediated by policies/rules on the University Firewall. • Users should ensure that their computer is virus free and has up to date anti-virus software installed. **Personally-managed computers connected via Ethernet port on the main campus** • Personally-managed equipment cannot be connected to the University wired network. Staff can appeal directly to the IT Support Manager, or to the manager of the School's IT support team. If these are unable to amicably resolve the matter, they should refer to the appropriate authority within their Faculty/School. **Personally-managed computers connected to a University-provided wireless network (e.g. Janet Roaming Service/eduroam)** • Student, staff and visitor managed computers will be registered by the owner using the 802.1x protocol during the process of making their connection - no further registration process is required. • As for all other personally managed equipment, access to authorised University services will be mediated by policies/rules on the University Firewall. • Users should ensure that their computer is virus free and has up to date anti-virus software installed. Users should be aware that both the UEA Conditions of Computer Use and the Janet Roaming Policy will be in effect whilst they are using this service.

GISP8. Offsite access control

Date:	5 October 2017
Version:	2.1
Document Owner:	Matt Roach
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
2.1	16/01/18	Reviewed by external auditor

Policy

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 unless appropriate not to, for example the web site.
Policy	8.1. All University computer systems will be protected against unauthorised connections from external computers (i.e. those not registered on the University's network). 8.2. Authorised connection to University computer systems from external computers will be available by VPN or will be enabled by rules on the firewall, which will be approved and configured according to defined policies and procedures 8.3. 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 8.4. Firewall and router rule sets must be reviewed at regular intervals each years.
Responsibility	• ITCS is responsible for maintaining the University firewall and for authorising any requests for external access to University systems. • ITCS is responsible for reviewing Firewall and router rules sets to ensure they are accurate, appropriate and that business justification has been documented.

	• ITCS will provide secure channels for connecting to computer systems. 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 Management	Any suspected breaches of the University's system access controls should be reported immediately to the IT Service Desk.
Audit and accountability	An annual review of all Firewall rules will be carried out by ITCS in consultation with Faculty/School/Unit IT support staff and other relevant authorities where appropriate. For systems within scope of PCI, reviews will take place at least every six months. Interim review of some specific rules will be carried out where those rules were indicated as 'temporary' at the time their creation was requested. Firewall logs will be inspected daily by ITCS staff for evidence of attacks and regular summary reports will be emailed to relevant IT support staff and service managers alerting them to the level and type of attacks on the service/system they are responsible for. ITCS will monitor network traffic and log any insecure connection methods (telnet, FTP etc.) being used. They will liaise with the relevant system administrators and IT support staff to ensure that use of such ceases and secure connection methods are used.
Implementation	**Firewall** • The Firewall will be set to deny all external connections to University computer systems, unless a rule on the Firewall permits access to the system via a specified Data Service (e.g. WWW, SMTP etc.). • Those Data Services which will be allowed to access internal systems via a specified port will be based on recommendations from Janet/CERT. • Requests for changes to Firewall rules in order to allow external access to Faculty/School/Unit systems, must be made by the nominated IT support person responsible for the security of the system(s). Such requests must be submitted in writing, with the awareness and approval of relevant authorities within the Faculty/School/Unit. Requests must include details of the access required, business justification for the request and the duration required for the rule. Where requests may affect specific working groups within a Faculty/School/Unit, the requester is expected to have made such working groups aware. • ITCS reserves the right to refuse requests if implementation of a request would pose a serious security threat to University systems/services. **Secure Connections** • ITCS will provide secure connection methods and client software for staff and student desktop computers for accessing email, connecting to central filestore (mapped network drives), file transfer and login access.

GISP9. Change management

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	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 GISP16). 9.3. System planning processes should explicitly define and document the legal obligations arising from the operation of the proposed system. There is a named individual responsible for updating that information. 9.4. Changes to operational procedures must be controlled to ensure on-going compliance with the requirements of information security and must have management approval. 9.5. Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software. All changes must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment.
Responsibility	• ITCS 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. • Service owners are responsible for ensuring on-going security compliance when undertaking any change.
Incident Management	If IT facilities/services are discovered to be insecure, this should be reported to ITCS, who will investigate and address matters with relevant project managers and stakeholders.
Implementation	• ITCS will define a process and develop templates to manage and record changes to services accounting for the impact on information security.

GISP10. Protection against malicious software

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	All computer systems must be protected against malicious software.
Objective	To prevent infection of all University computer systems by malicious software such as viruses, trojans, worms, key loggers etc.
Policy	10.1. All devices connected to the University network must have up to date security patches installed, and be configured to update automatically using ITCS provided central mechanisms wherever possible. 10.2. All devices connected to the University network must have University approved software installed that will protect against malicious software such as viruses, Trojans, worms, key loggers etc. where feasible. The software and associated data files should be installed and configured following defined policies and procedures. 10.3. All systems connected to the University internal managed network will be regularly scanned for vulnerabilities. All high risk vulnerabilities discovered must be resolved within 30 days (e.g. by installation of a security patch).
Responsibility	• ITCS 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. • All users have a responsibility for protecting against malicious software and particular care and vigilance should be taken when downloading files from untrusted sources.

Incident Management	• Any computer system found to be infected with malicious software will be disconnected from the network until the software has been 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.
Audit and accountability	IT Support Managers should ensure that a security audit of systems in their charge is carried out on a regular basis (at least annually) and remedial action undertaken where necessary.
Implementation	**Operating systems** • Computers running multiple operating systems, either via dual boot mechanisms, emulation, or virtual machines, should ensure that each operating system has up to date patches, security packs, anti-malware software installed, all of which should be automatically updated wherever possible. **Application software suites** • All application software suites should have the latest patches and security packs installed and wherever possible ensure that auto-update mechanisms for these are in place. **Firewall** • All operating systems should have their firewall switched on and any exceptions to the default firewall rule set are only to be allowed by agreement with IT support. **Anti-virus and anti-malware** • Anti-virus and anti-malware software should be installed and kept up to date. Auto update mechanisms for virus definitions etc. should be enabled. **Securing desktop computers against unauthorised access** • The number of local and privileged user accounts on workstations must be kept to an absolute minimum. • No workstations should allow remote access to any non-University members without prior permission from ITCS. • Users should not normally access workstations using accounts that have elevated privileges, except in specific cases where required by IT support – see GISP5 ‘Desktop local administrator accounts’. • Where elevated privileges to a computer have been requested and approved for a user, these should be enabled by IT Support staff using Active Directory group policies wherever possible and assigning specific rights for a user on a specific machine. • When a user leaves UEA employment or changes their roles/responsibilities any access rights or local accounts assigned to that user should be removed or modified as appropriate.

GISP11. Information classification

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	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. 11.2. Classified information and outputs from systems handling classified data must be appropriately labelled according to the output medium. 11.3. Damaged storage devices containing sensitive data will undergo appropriate risk assessment, to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of the organisation and only be removed from site with the permission of the information asset owner. 11.4. All employees to be aware of the risk of breaching confidentiality associated with the photocopying (or other duplication) of sensitive documents. Authorisation from the document owner should be obtained where documents are classified as Confidential or above. 11.5. Any third party used for external disposal of the organisation's obsolete information-bearing equipment or hardcopy material must be able to demonstrate compliance with this organisation's information security policies and also, where appropriate, provide a Service Level Agreement which documents the performance expected and the remedies available in case of non-compliance. 11.6. Prior to sending sensitive information or documents to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party, must continue to assure the confidentiality and integrity of the information. 11.7. Sensitive or confidential data should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.

Responsibility	• ITCS 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 Management	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.
Implementation	• The University's information classification scheme and guidance on its application to data is available from https://portal.uea.ac.uk/documents/6207125/6857482/Information+classification+policy.pdf. This policy includes definitions of the following terms: information asset, data owner, data administrator, and data management.

GISP12. Secure areas

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	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. 12.3. Where sensitive data is stored in secure areas, network access to that data must be carefully controlled and monitored following documented procedures. 12.4. Sensitive data supplied by third parties must be stored in secure areas in compliance with the agreement with the third party. 12.5. 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 Management	• 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.
Incident management	Where IT security of a secure area is found/judged to be inadequate, this should be reported immediately to the manager for that area.

	Where IT security mechanisms are discovered to have been breached, the manager of the area should liaise with ITCS and other University agencies as appropriate and take the necessary action to remove/reduce any security threats. Details of the incident should be recorded, including times/dates, relevant system logs and actions taken. If the breach is considered to have been a major one, with significant impact on data and services, a full report should be submitted to Faculty management or ITCS Divisional Directors as appropriate. The Security Risk log should also be reviewed in light of such incidents.
Audit and accountability	Managers of the secure areas should audit IT security of the areas on a regular basis (at least annually), taking remedial action as appropriate. Outstanding issues and deviation from these controls should be recorded in the annual Security Policies Implementation Issues Log which is collated by ITCS and submitted to ISSC for review.
Implementation	• A manager of the secure area should be nominated and they will be responsible for all aspects of the area's security (physical and IT security) • Physical security controls should be applied – see GISP3. • Data associated with the secure area should be stored and handled in accordance with security controls/ policies detailed in the Information Classification and Data Management Policy. • There may also be additional data controls/policies as applied by a funding agency that must be abided by. • Only secure encrypted data channels should be used to connect to systems and data, except where insecure data protocols are implicit within the service, e.g. HTTP for web services. • It should be ensured that the necessary University Firewall policies are in place to protect against unauthorised external access to systems, see GISP8. • It should be ensured that all systems operated from, or stored within the secure area are appropriately protected against unauthorised user access by complying with policies and security controls as listed below: GISP4. Identification, authentication and authorisation GISP5. Use of passwords • It should be ensured that the segment of network used for the secure area is appropriately protected against unauthorised access via the University network. Where appropriate this may mean a separate subnet being used for the secure area and/or use of the University Firewall policies to mediate access. The appropriate mechanisms should be determined by agreement with ITCS Network Services. • All network connected equipment used within the secure area, or used to connect to the secure area, should comply with University equipment registration security controls and policies. • A Security Risk Log for services/systems operating from the secure area should be created and reviewed on a regular basis (at least annually).

GISP13. Business continuity and disaster recovery

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	A Disaster Recovery Plan will be in place to protect the University's business processes and information assets from loss or failure of IT or telecommunications services.
Objective	• To ensure that in the case of a failure or disaster affecting University IT services or telecommunications, a plan for service recovery exists. • To ensure that in the case of a major failure or disaster affecting University IT services or telecommunications, a plan for continuing to deliver business processes exists and is aligned to recovery times. • To ensure that University information assets are stored securely and can be recovered in the event of loss.
Policy	13.1. A Disaster Recovery Plan (including system backup and restoration facilities as appropriate) 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. 13.3. All staff must be made aware of the business continuity plan and their own respective roles. 13.4. Information owners must ensure that appropriate backup and system recovery procedures are in place. 13.5. Management must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files; especially where such files may replace more recent files. 13.6. Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

	13.7. All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary should be applied by management and determined by the classification of the information in question. 13.8. Highly sensitive or critical documents should not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports should normally be self-contained and contain all the necessary information.
Responsibility	ITCS is responsible for maintaining and reviewing a Disaster Recovery Plan. ITCS is responsible for establishing and running backup regimes which allow for recovery of systems in line with the Disaster Recovery Plan.
Incident Management	In the event of a major catastrophe affecting IT or telecommunication systems, the Disaster Recovery Plan will be consulted and appropriate action taken.
Audit and accountability	Managers of the systems should audit disaster recovery plans on a regular basis (at least annually), taking remedial action as appropriate. Outstanding issues and deviation from these controls should be recorded in the annual Security Policies Implementation Issues Log which is collated by ITCS and submitted to ISSC for review.
Implementation	**Minimum requirements for safe/secure data storage** • All University owned computer systems should be secure against unauthorised access to data stored on them and compliant with the University's Information Security Policy. • Data should be copied/backed up at least once every 24hrs to a safe and secure location/media away from the desktop. • Exception is data generated temporarily during local processing operations. • The backing up of data from computers should be independent of end-user action and mechanisms should be in place to enable automated synchronisation of stored data with the backup copy. • University owned laptops when connected to campus network should operate under the same policies as for static desktop systems, but the backing up of data from such systems may require end-user action. • All data backups should be secure against fire, theft, flood and unauthorised access, and compliant with the University's Information Security Policy. • Any data utilised, or generated by strategic corporate information systems (e.g. finance and personnel systems) should be stored only on the centrally provided storage associated with those systems.

	• Exception is where centrally provided corporate systems cannot provide all reports required to comply with funding and regulatory bodies, or for University management purposes, it may be necessary to process and store some data on the desktop. This data should be backed up to a secure location/media. • If data is to be shared with other individuals/groups the data should be shared from another secure location such as central filestore or Office 365 so that data access is not compromised due to the desktop system being out of service. All such shared resources should have appropriate security measures in place to prevent unauthorised access to data and comply with the University Information Security Policy. • Anonymous FTP should not be used to share desktop computer data. **Central provision for storage of desktop data** • ITCS will provide safe, secure and backed up central filestore with individual quotas for staff and students to store their work data. This filestore will have no single point of failure and hence will be highly available. • Filestore quota will be "fit for purpose" and sufficient for the storage of work data for the majority of staff and students. • Exception is where a researcher requires large amounts of storage the central filestore quota may be insufficient and additional arrangements as defined will have to be made. • Staff and student quotas will be published on ITCS's web pages. These quotas will be reviewed annually in consultation with Faculties/Schools/Units with the aim of ensuring that quotas keep pace with the demand. However, it should be realised that the quotas offered may be constrained by the level of available funding. • Mechanisms will be provided for individuals, working groups and Schools/Units to purchase or rent additional storage on the central filestore system. These mechanisms will be published on ITCS's web pages. • All desktop data stored on central filestore will be backed up to a secure location on a 24hr basis. Backups will be retained for a guaranteed period. • Where data is required to be kept for a prolonged period of time, the user should consider long-term archive arrangements. • Files will be available from backup for restore to a user's central filestore. Arrangements and procedures for restoring files will be documented on ITCS's web pages. • ITCS will provide mechanisms to allow PC, Mac, UNIX and Linux desktop systems to connect to central filestore in such a manner that the filestore appears as a 'native' drive or folder on that system. • ITCS developed Standard Staff and Student Desktops will provide an automatic connection to the user's central filestore and synchronisation at regular intervals between locally cached data and the central copy, including at logon and logoff.

	• Provision will be made for sharing of centrally stored data between individuals and groups connected to the campus network. Such provision will allow for fine control of access down to the user and file level.

GISP14. Incident reporting and handling

Date:	5 October 2017
Version:	2.1
Document Owner:	Matt Roach
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
2.1	18/01/18	Review by External Auditor

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. For systems covered by PCI DSS there is a requirement under 12.10.1 which states that a security incident plan and a set of pre-defined responses are documented and practiced. These are not publically available. In addition, in the event of an incident, payment brand procedures must be follow and requirements met. 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 Information Compliance Team 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** • • The Security Incident response plan and if appropriate the pre-defined incident response procedures should be followed (see reference to separate document "security incident response plan") **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** • Follow the steps documented in the Security Incident Response Plan and if appropriate the pre-defined incident response procedures (see reference to separate document "security incident response plan")

	• . **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 Data Protection Officer, who will take appropriate action which may need to involve external agencies.

GISP15. Network monitoring

Date:	5 October 2017
Version:	2.1
Document Owner:	Matt Roach
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
2.1	16/01/18	Review by external auditor

Policy

Security Control	Monitoring and logging of network traffic to identify security threats and to maintain the highest levels of service for all users.
Objective	To ensure that network traffic is monitored and logged in order to detect activity in breach of this General Information Security Policy and/or the Conditions of Computer Use and to ensure use of the network does not disrupt service to end users.
Policy	15.1. Regular monitoring and logging 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. 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, is in breach of the Conditions of Computer Use or if there are allegations of misconduct. 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. Where wireless devices not authorised by ITCS cause interference and service degradation to the University wireless network service, the University reserves the right to require the removal of the equipment. 15.5. Various activities on the network, including websites visited, may be routinely logged for diagnostic and evidential purposes.

Responsibility	ITCS is responsible for monitoring and logging 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 Management	Incidents detected by network monitoring and logging will be reported to the Information Compliance team in ITCS 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. Legal and regulatory compliance

Date:	5 October 2017
Version:	2.1
Document Owner:	Matt Roach
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
2.1	18/01/18	Review by external auditor

Policy

Security Control	All use of information systems and assets will comply with current legislation.
Objective	• To ensure that all University IT and computing systems comply with current legislation. • To ensure that information is managed in such a way as to ensure compliance with current legislation. • To ensure that use of the University network is in accordance with regulations of the Joint Academic Network (Janet) and security standards of the Payment Card Industry (PCI).
Policy	16.1. All University IT and computing systems and information services hosted on these must be compliant with current legislation. 16.2. All use of the University network and its connections to the internet must be compliant with Janet regulations. 16.3. All systems connected to the University network falling within the scope of PCI must be compliant with the PCI Data Security Standard (DSS). These requirements are covered by the Face to Face & MOTO card payment security policy and the E-commerce security policy. 16.4. All systems both those run by the University and by third parties which process personal data must be compliant with the expectations of data protection legislation. 16.5. The terms and conditions of the institution provisioning the IT account apply to the use of the account through the host connection, e.g. where an academic visitor uses a UEA connection via eduroam. 16.6. System or service planning process should explicitly define legal obligations. 16.7. The University will have a Records Management Policy and relevant Information Compliance policies.

	16.8. A nominated person is responsible for preparing guidelines to ensure that all staff and students are aware of the key aspects of the law of copyright, in so far as these requirements impact on their duties or studies. 16.9. A formal security awareness program in place to make all personnel aware of the PCI DSS cardholder data security policy and procedures.
Responsibility	• ITCS is responsible for making users, system administrators and data owners aware of legislation and regulations with which they must comply. • The Finance Division is responsible for making users, system administrators and data owners aware of PCI regulations 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 and regulations.
Incident Management	Where it is suspected that a computer system, service or activity does not comply with legislation or regulations, the matter should be reported to the owner of the system or service involved. Legal and regulatory breaches should be reported to the Strategy, Policy and Compliance team. For incidents relating to PCI, a defined security incident response plan will be followed.
Audit and accountability	The Information Compliance team are responsible for record keeping, liaison with appropriate authorities and internal departments, and will provide a report on breaches to ISSC on an annual basis.
Implementation	• To support compliance with information legislation, all data owners will ensure that the records held are managed in accordance with the University's records management policy and there exist associated records retention policies and supporting departmental processes to effect them. See https://portal.uea.ac.uk/documents/6207125/7105351/Records-Management-Policy.pdf • Information regulations and policies are available from https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies • All systems that fall within the scope of PCI will adhere to the data security standards required under the relevant PCI SAQ level.

GISP17. IT and information asset management

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	Ensuring University IT and information assets are known, and access to these assets is managed.
Objective	• To ensure that the University is fully aware of all IT equipment and software assets it owns and there is a registered owner responsible for each asset. • To ensure that the University is fully aware of all information assets 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 the Information Classification and Data Management policy.
Policy	17.1. 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. 17.2. Information assets should be classified according to the Information Classification and Data Management policy. 17.3. 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).
Responsibility	• Each Faculty or service unit is responsible for ensuring an inventory is in place for the assets it owns, and that the inventory is regularly reviewed to ensure that the records held remain accurate. • For departments where IT is managed by ITCS, it is responsibility of the ITCS managed IT technicians to maintain an up-to-date IT asset inventory for the department.

	• For other departments where the IT is not managed by ITCS, it is the responsibility of the department to maintain an up-to-date IT asset inventory for the department. • In either case, it is the responsibility of the department to maintain up-to-date inventories of the information assets it owns. • Those specified above who are responsible for the asset inventory will make this available to appropriate authorities within the University on request.
Incident Management	Where an information asset has been compromised, the owner of that asset should be notified. Further action is as defined by GISP14. Where an IT or information asset is not recorded in an inventory, the manager with responsibility for the asset should provide the IT Support Manager with appropriate details.

GISP18. Encryption use and key material handling

Date:	5 October 2017
Version:	2.1
Document Owner:	Matt Roach
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
2.1	18/01/18	Review by External Auditor

Policy

Security Control	Control of encryption use by staff, students, and visitors.
Objective	• To ensure that encryption is used in a consistent and manageable manner and applied only to Confidential or Secret Information Classes as defined in the Information Classification and Data Management policy. • To ensure the ability to undertake University work is not adversely affected by the use of encryption. • To ensure that appropriate encryption methods are in use for the transmission of cardholder data.
Policy	18.1. Use of encryption to protect cardholder data transmission will be used for all systems within scope for PCI DSS. 18.2. Use of encryption to protect University data should be in accordance with the University's policies on information classification. 18.3. Where encryption is used the encryption method used should follow University defined procedures. 18.4. When encryption is used, details of the encryption method and keys should be securely stored and accessible to the user's line manager or supervisor.
Responsibility	• ITCS is responsible for determining and publishing procedures and guidelines for using encryption. • For systems within scope of PCI DSS ITCS will determine and put in place operational procedures and documented guidance on the use of encryption for all cardholder data transmission. • 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 Management	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.
Audit and accountability	ITCS should review any encryption services they provide on a regular basis (at least annually), checking against these policies/controls and recognised best practice, and taking remedial action as appropriate. Outstanding issues and deviation from these controls that are judged to present a significant security risk should be recorded in a Security Risk Log.
Implementation	**General** • University data (including files and emails) should only be encrypted where there is a need to protect secret, sensitive or confidential data against unauthorised access and in accordance with the UEA Information Classification and Data Management policy. • Decryption keys should be stored securely and arrangements made wherever possible for managers to access the keys when personnel are absent and lack of access to the data is preventing/hindering pursuance of UEA work. The keys must also be made available to the relevant authorities during any investigation of criminal activity or financial irregularities. **Encrypted data channels and protocols** • Where IT account authentication data such as usernames and passwords are transmitted over the network, for instance in order to connect to a service or open a channel for data transfer, that data should be transmitted in an encrypted format wherever possible following best practice and based on strong encryption following current industry best practice. • University email clients should use secure protocols as provided by University provided and approved secure email services. Where web services are used to access University email, only the secure https protocol should be used (not http). • Where cardholder data is transmitted as part of in-scope PCI DSS systems these transmission channels must be encrypted following industry best practice and based on strong encryption. • Only secure protocols should be used (TLS, IPSEC, SSH, etc.). Insecure versions or configurations must not be used (SSL or early TLS). • Where confidential or sensitive data is being transmitted using web services, the secure https protocol should be used. • Server to server data feeds should all be encrypted wherever possible. • Where members of the University are working in countries which ban or impose severe limitations on use of encryption, the University may not be able to provide encrypted data channels and alternative mechanisms may have to be used. In such cases care should still be taken to ensure good data security. **File encryption** • File encryption used should be based on strong encryption following current industry best practice[5]. • Sensitive or confidential data should only be stored on mobile devices where it is essential to do so. Storage of such data on portable computers or USB storage devices should always be encrypted. Storage on other mobile devices such as portable phones should be encrypted, or at the least access to the device password protected, wherever possible.

[5] Note, if Microsoft Office documents are saved with the encryption option selected, this is the default setting.

	• Advice on encrypting Microsoft Office documents is provided in the helpsheet available from https://portal.uea.ac.uk/is/online-wiki-helpdesk/-/wiki/Main/How+to+encrypt+a+Microsoft+Office+document • Advice on creating an encrypted archive containing files of any type is available from https://portal.uea.ac.uk/documents/6207125/6857482/Encrypt%2Ba%2Bfile.pdf **Email encryption and digital signatures** • Encryption when used should be based on strong encryption following current industry best practice and public and private keys (e.g. the PGP and S/MIME models). • Digital certificates used to verify identity of the sender will be provided via the UEA staff email service for both internal and external email communications where required. **End-user messaging technologies** • Where secret, sensitive or confidential information is transmitted via end-user messaging technologies such as email, instant messaging, SMS or chat, it must be sent using strong encryption following current industry best practice. • In particular, the PCI-DSS requires that unencrypted Primary Account Numbers (PAN) are not sent via end-user messaging technologies.

GISP19. Personnel security

Date:	5 October 2017
Version:	2.1
Document Owner:	Matt Roach
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
2.1	18/01/18	Review by External Auditors

Policy

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 misuse is minimised.
Policy	19.1. Where appropriate to the post, staff job descriptions should contain details of information security roles and responsibilities. 19.2. 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. 19.3. All employees are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after their employment with the organisation. 19.4. All staff with information processing duties will receive appropriate guidelines and training in regard to information security and compliance. 19.5. Training in information security threats and safeguards for technical staff is mandatory, with the extent of technical training to reflect the job holder's individual responsibility for configuring and maintaining information security safeguards. Where IT staff change jobs, their information security needs must be reassessed and any new training provided as a priority. 19.6. Staff with responsibility for system administration will have training in secure system configuration. 19.7. Staff should only have access to information that is required for the role.

	19.8. Persons responsible for Human Resources management are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organisation and to external parties. 19.9. When roles change, procedures should be followed to ensure that access rights are reviewed. 19.10. Management must respond quickly yet discreetly to indications of staff disaffection, liaising as necessary with Human Resources management and the Information Compliance Team. 19.11. Departing staff are to be treated sensitively, particularly with regard to the termination of their access privileges. 19.12. On termination of employment, procedures should be followed to ensure that all access rights to University information or information processing facilities are removed. 19.13. Departing staff must return all information assets and equipment belonging to the organisation, unless agreed otherwise with the designated owner responsible for the information asset. 19.14. Periodic training for appropriate staff within the Information Compliance Team is to be prioritised to educate and train in the latest threats and information security techniques.
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. • ITCS are responsible for ensuring that all staff are reminded of information security and compliance matters on an annual basis. • 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 Management	If it is suspected that the above controls/policies have not been followed, the matter should be reported to HRD.

GISP20. Personally-owned equipment terms and conditions

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	Terms and conditions of personally-owned equipment connections to the University's wired and wireless data network.
Objective	• To ensure all personally-owned computer systems connected to the University's data network are done so in accordance with relevant legislation and regulations. • To ensure all personally-owned computer systems connected to the University's data network pose a minimal security risk to services and other users on the network.
Policy	20.1. The University reserves the right to disconnect any network access point within residences or access via the wireless network, and take appropriate further action, where its use has contravened the above terms and conditions.
Responsibility	• ITCS is responsible for maintaining and publicising the means of connecting personally-owned equipment 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. • Individual users are responsible for the use of equipment registered onto the network in their name whenever it is in use.
Incident Management	Where it is discovered that a network connection is being used in contravention of this policy, access to the network will be suspended and further action taken.

GISP21. Liability of own systems and content brought to University

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	Controls to ensure that personally-owned devices connecting to the University network do not compromise security, or introduce liabilities for the University.
Objective	To ensure that personally-owned devices connected to the University network do not compromise security or give rise to any claims against the University.
Policy	21.1. All connections to the wireless network must be authenticated using valid credentials. See GISP7. 21.2. All personally owned equipment connecting to the wired network (including residences) must be registered before connection is permitted. See GISP7. 21.3. The University accepts no responsibility for either the safety or security of personally owned systems.
Responsibility	• ITCS is responsible for providing a secure network and method of connection for personally owned equipment. • Users are responsible for ensuring their personal computer systems are safe, secure and operated within legal frameworks.
Incident Management	Incidents should be reported to the IT Service Desk. If a personally 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.

GISP22. Working with third parties

Date:	5 October 2017
Version:	2.1
Document Owner:	Matt Roach
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
2.1	18/01/18	Reviewed by External Auditor

Policy

Security Control	Controls to maintain security of the University's information and systems when third parties, i.e. those other than University staff or students, are involved in their operation.
Objective	To ensure that information security is considered and risks minimised when the University works with contractors involved in the design, development or operation of information systems, or when users who are not members of the University are given access to information or information systems.
Policy	22.1. All contracts with external suppliers for the supply of services to the organisation must be monitored and reviewed annually to ensure that information security requirements are being satisfied. Contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier and must be complete with contact details of all personnel concerned. 22.2. Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the contents and spirit of the organisation's information security policies. 22.3. Persons responsible for commissioning outsourced development of computer based systems and services must exercise due diligence and use reputable companies that operate in accordance with quality standards and which will follow the information security policies of this organisation, in particular those relating to application development.

	22.4. Where responsibility for maintaining security standards is shared between the external supplier and the University, the agreement shall detail where the responsibility lies (with the supplier or the University). 22.5. All external suppliers who are contracted to supply services to the organisation must agree to follow the information security policies of the organisation. An appropriate summary of the information security policies must be formally delivered to any such supplier, prior to any supply of services. 22.6. Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is important. 22.7. An appropriate summary of the information security policies must be formally delivered to any contractor, prior to any supply of services. 22.8. An appropriate summary of the information security policies must be formally delivered to, and accepted by, all temporary staff, prior to their starting any work for the organisation. 22.9. Any facilities management, outsourcing or similar company with which this organisation may do business must be able to demonstrate compliance with this organisation's information security policies and enter in to binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.
Responsibility	• Data and system owners will assess the risk to its information posed by providing third party access before granting access. Where necessary, data and system owners will require third parties to sign confidentiality agreements to protect the information assets. • ITCS is responsible for ensuring that service or support and maintenance agreements with third parties are in accord with the University's information security policies. • Third parties are responsible for ensuring their computer systems are safe, secure and operated within legal frameworks and used in accordance with this security policy and the Conditions of Computer Use. • All third parties given access to University information systems must agree to follow the University information security policies.
Incident Management	Incidents should be reported to the IT Service Desk in the first instance for investigation by the Information Compliance Team as described in GISP14.

GISP23. Mobile devices

Date:	5 October 2017
Version:	2.0
Document Owner:	Matt Roach
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	Controls to minimise the risk of loss of University information assets when using mobile devices such as laptops, mobile phones, data sticks or removable storage or accessing University systems when off site and located at non-University premises.
Objective	To ensure that security is added to mobile devices to prevent unauthorised access and maintain confidentiality. To ensure that all information systems and assets are assessed as to their suitability for mobile or off site access before such access is granted.
Policy	23.1. Persons who will be doing part or all of their work using dedicated equipment in a fixed location outside the organisation (teleworking) must be authorised to do so by an appropriate authority within the organisation. A risk assessment based on the criticality of the information assets being used and the appropriateness of the proposed teleworking location should be carried out. 23.2. Teleworkers will be provided with appropriate computing and communications equipment and must use only this equipment for teleworking. The equipment provided may only be modified or replaced if this has been authorised. All equipment must be returned at the end of the teleworking arrangement, or when the teleworker leaves the organisation. 23.3. All teleworking agreements must include appropriate measures, based on a risk assessment, to protect the security of information assets. Teleworkers must follow the agreed security procedures at all times. 23.4. All teleworking agreements must include rules on the use of equipment provided for teleworking. Teleworkers must abide by these rules at all times unless specifically authorised. 23.5. Persons accessing information systems remotely to support business activities must be authorised to do so by their line manager or the system owner for the information system (as appropriate). A risk assessment based on the criticality of the information asset being used must be carried out. 23.6. Utmost care must be used when transporting files on removable media (e.g. disks, portable HDs, CD-ROMs and USB flash drives) to ensure that valid files are not overwritten and incorrect or out of date information is not imported.

	23.7. The University will publish guidelines for users of mobile computing equipment advising them on how these should be used to conform to the information security policies and other good practices.
Responsibility	• ITCS is responsible for ensuring access to services by mobile devices is secured where possible, or unable to be accessed where no security option is available. • ITCS is responsible for providing guidance on good practice in the use of mobile devices. • Users are responsible for ensuring that their use of mobile devices or remote facilities is in accordance with good practice advice and the information security policies.
Incident Management	Incidents should be reported to the IT Service Desk for further investigation.
Implementation	**Exchange mobile device security** An Exchange Security Policy should be applied to all mobile devices which synchronise with Exchange. The following settings for the policy should be applied: • Mobile device requires passcode • Minimum passcode length = 6 • Number of failed pass-code attempts until device is reset to factory default (formatted) = Maximum available[6] • Time without user input after which passcode must be re-entered (in minutes) = 5 • Enforce passcode history (remembers last 3 passcodes) • Require encryption on the storage card • Enable passcode recovery (user can obtain recovery passcode via OWA). • Enable a remote wipe facility for devices that synchronise to UEA email using ActiveSync. This can be used in the event that a device is lost or stolen and can be activated by the owner of the device through OWA. • In extreme circumstances, a remote wipe of a lost or stolen device can be performed by ITCS but only with the explicit consent of the device owner. **Guidelines on use of mobile devices** Guidance on setting up security on a mobile device (phone or tablet) accessing the University email service is available from the ITCS web site at: https://portal.uea.ac.uk/documents/6207125/7752191/11.+Mobile+Device+Security-v1.pdf/

[6] Maximum no. of failed attempts available = 16

GISP24. Systems management and development

Date:	5 October 2017
Version:	3.1
Document Owner:	Matt Roach
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
2.0	1/2/13	Inactivity timeout addition approved by ISSC
2.1	5/10/17	Reviewed and updated
3.0	20/10/17	Approved by ISSC
3.1	16/01/18	Review by External Auditors

Policy

Security Control	Control of the installation, configuration, maintenance, development and management of information systems and the software and services they run.
Objective	To ensure that information security good practice is applied to the installation, configuration, maintenance, development and management of information systems.
Policy	24.1. The organisation's systems must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the organisation's information security. 24.2. All systems must be regularly checked to ensure that they comply with the organisational security policy. 24.3. The procedures for the operation and administration of the organisation's business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained. Procedures for developing and maintaining secure systems within PCI scope must be documented, in-use and known to affected parties. All systems must have secure configurations applied to approved industry best practice standards.

	24.4. Procedures will be established for the reporting of software malfunctions, threats, vulnerabilities and faults in the organisation's information processing systems. Faults, threats, vulnerabilities and malfunctions shall be logged and monitored and timely corrective action taken. For public facing web applications within scope of PCI new threats and vulnerabilities must be assessed on an ongoing basis using approved vulnerability scanning tools. New threats and vulnerabilities should be corrected and systems re-evaluated or an automated solution which detects and prevents web-based attacks. 24.5. Development and testing facilities for business critical systems shall be separated from operational facilities and the migration of software from development to operational status shall be subject to formal change control procedures. 24.6. Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place. 24.7. Procedures shall be established to control the development or implementation of all operational software. All systems developed for or within the organisation must follow a formalised development process. All staff performing development on PCI related systems will receive annual training in secure coding techniques. 24.8. A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals. 24.9. New information systems, or enhancements to existing systems, must be authorised jointly by the manager(s) responsible for the information and the Assistant CIS Director. The business requirements of all authorised systems must specify requirements for security controls. 24.10. The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the Information Classification and Data Management policy, and a risk assessment undertaken to identify the probability and impact of security failure. 24.11. Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the organisation's information security policies, access control standards and requirements for on-going information security management.

	24.12. Systems must be configured to industry-accepted security hardening standards. Before installation on the network, all vendor supplied defaults must be changed, and all unnecessary default accounts must be removed or disabled. 24.13. Systems handling payment card details (in the cardholder data environment), handling personal data, or forming part of the institution's key infrastructure must be subject to regular penetration testing by suitably qualified personnel following an agreed methodology. Penetration testing should be conducted at least annually, or after any significant infrastructure or application upgrade. 24.14. The organisation's systems are to be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with nominated individual system owners. All systems management staff shall be given relevant training in information security issues. 24.15. Security event logs, operational audit logs and error logs must be properly reviewed and managed by qualified staff. Logs must record all actions by users with root or administrative privileges, invalid logical access attempts, and use of or and changes to authentication mechanisms. Logs must be written to a secure, internal log server. Any anomalies or suspicious behaviour identified must be followed up. 24.16. The procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by the organisation must always follow a formalised development process. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls. 24.17. Inactive connections to the organisation's business systems shall shut down after a defined period of inactivity to prevent access by unauthorised persons.
Responsibility	• Data and system owners are responsible for ensuring their data and system is managed in accordance with the University's information security policies. • ITCS is responsible for ensuring all staff managing information services are managed by suitably trained and qualified staff.
Incident Management	Incidents should be reported to the IT Service Desk in the first instance who will escalate the incident as appropriate.
Implementation	Further information about information systems managed by ITCS is available from the ITCS web site at https://portal.uea.ac.uk/itservices/corporate-systems.

	See also GISP9 Change management. **Inactivity timeout period** When the system is implemented, ITCS will seek agreement with the system owner on an appropriate period of inactivity before automatic logout. The following points should be considered when deciding this period: • Whether auto logout of the system is supported by the system • Whether different periods are supported by the system for different user circumstances. If not, then the minimum required period will be applied to all users • The period should account for the risk of unauthorised access associated with the location of the computers accessing the system (e.g. whether they are located in publically accessible spaces) and the information classification of the information held on the system • The period should account for its impact on day to day activities. **<u>Systems and Applications in scope for PCI</u>** Staff with responsibility for developing code must be trained at least annually in secure coding techniques, including avoidance of common coding vulnerabilities and the handling of personal data in memory. Coding techniques must address: • Injection flaws (SQL, OS and LDAP injection) • Buffer overflows • Insecure communications • Improper error handling • All high risk vulnerabilities identified in the vulnerability identification process • Cross-site scripting • Improper access control • Cross-site request forgery • Broken authentication and session management For public-facing web applications, new threats and vulnerabilities must be addressed on an ongoing basis. This can be done by running application vulnerability security assessment tools annually or after every change. The tool can be run by an organisation that specialises in application security. All vulnerabilities must be corrected and the application re-evaluated after corrections. Alternatively installation of an automated solution which detects and prevents web-based attacks can take place. This should be located in front of public-facing web applications, actively running, generating audit logs and configured to block web-based attacks or generate an alert which is investigated.