University of Sunderland – Business Assurance
Information Security Policy

Document Classification: **Public**

Policy Reference – Central Register	_____
Policy Reference – Faculty / Service	IG 003
Policy Owner	Director of Business Assurance
Date Policy Written	May 2013
Author	Assurance Manager, Business Assurance
Date Policy Last Updated	
Date to Information Governance Group	13th June 2013
Date to Executive	26th July 2013
Date for next Review	December 2016
Comments	

Information Security Policy

Contents

Information Security Policy

1. INTRODUCTION

Information Security is concerned with all information, in electronic and paper format and spoken. The main purpose of implementing good information security is to allow the effective and efficient use of information, whilst safeguarding the organisation's data from unauthorised access or modification, to ensure its availability, confidentiality and integrity.

This high-level information security policy is a key component of the University's overall information governance framework and should be considered alongside more detailed information governance documentation including, system level security policies, security guidance and protocols or procedures.

2. PURPOSE AND SCOPE

The aim of this policy is to advise staff and contractors of their obligations with regards to confidentiality and where to seek further guidance and assistance.

This policy applies to all University staff, independent contractors and students.

It applies to all information, information systems, networks, locations and applications.

The objectives of the Information Security Policy are to preserve:

- **Confidentiality** - Access to data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

3. DEFINITIONS

3.1. System Level Security Policies (SLSPs)

Documentation specific to a system, covering security and management procedures in place throughout for data collection, data handling, data storage, data analysis and data destruction.

3.2. Information Security Management System (ISMS)

The governing principle behind an ISMS is that an organisation should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.

3.3. Information Asset

Information held which is of value to an organisation. This includes (but not exclusively) statutory, financial and commercial information..

Further guidance will be available in the University's Information Risk Management policy and associated guidance documents.

3.4. Information Security Incident

An information security incident is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy. This could involve a breach of the Data Protection Act 1998 where the incident concerns personal data.

4. DUTIES AND RESPONSIBILITIES

Overall responsibility for this policy lies with the Director of Business Assurance, who performs the role of the University's Senior Information Risk Owner (SIRO)
The SIRO is responsible for:

- Ensuring that an overall culture exists that values and protects information within the organisation
- Owning the organisation's overall information risk policy and risk assessment process, testing its outcome and ensuring that it is used
- Owning the organisation's information incident management framework

The Assurance Manager (Business Assurance - Information Governance), responsible to the Director for Business Assurance, is responsible for drawing up information governance and information security policy, process and guidance for good information security practice and ensuring compliance with this policy.

The **IT Security Manager (ITS),** reporting to the Assistant Head of Technology Services, is responsible for developing IT Security Policy, standards and guidelines. He/she is also responsible for ensuring that effective IT Security systems, controls and training programs are operationally implemented, fit for purpose and available across the University.

The **Legal Support & Data Protection Officer** is responsible for developing policy, process and guidance relating to Data Protection and can provide advice on collecting, using and protecting personal information.

The University Deans of Faculty and Directors of Support Services have responsibility for ensuring compliance with the University's Information Governance policies and ensuring any issues of non-compliance are addressed. They have responsibility for ensuring that an appropriate member of staff, in each Faculty and Service, takes on the role of "Information Champion".

The Information Governance Group is responsible for recommending policy direction on records management to the Executive and monitoring that agreed policies are followed.

Information Champions are accountable to their Dean of Faculty/Director of Service and have a responsibility to monitor information security compliance and awareness and be the

primary point of contact and source of information and support within the Faculty/Service. The Information Champions Group will report to the Information Governance Group.

Individual employees, students and 3rd party contractors have responsibility for ensuring that they comply with this policy and any related policies and guidance. Staff should attend training and awareness sessions provided by the University. Employees also have a duty to report any incidents or 'near misses' in relation to information security.

5. POLICY DETAILS

5.1. Governance and Assurance

Information Security Awareness\Training

Information security awareness training shall be included in the staff induction process. An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

Contracts of Employment

Information security expectations of staff shall be included within appropriate job definitions.

Third party services

All contracts regarding outsourced IT systems and handling of data will include:

- information security requirements, including confidentiality, integrity and availability,
- a description of the agreed security level,
- requirements for reporting security incidents from third parties,
- a description of how the University may ensure that third parties are fulfilling their contracts,
- a description of the University's right to audit third parties.
- an agreement by the third party to be subject to an annual Supplier Information Security Assessment (SISA)

Security Control of Assets

Each information asset shall have a named Information Asset Owner who shall be responsible for the information security of that asset.
The level of protection offered to the asset will be appropriate to the classification of the information held and the potential risk to the asset.

The University's Information Risk Management policy should be consulted for further information.

In order to minimise loss of, or damage to, all assets, equipment, including IT, shall be physically protected from threats and environmental hazards.

Physical Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data, including both physical records and electronic records.

Information Risk Management

A formal information risk management approach will be implemented by University of Sunderland.

For each information asset, information security risks will be identified and quantified in terms of the perceived value of the information asset, severity of impact and the likelihood of occurrence.

The Information Risk Management policy should be consulted for further information.

Information Security Incidents and weaknesses

All information security events and suspected weaknesses are to be reported to in line with the Incident Response Plan.. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules of the relevant jurisdiction.

Classification of Information.

Information will be classified based on the perceived value of the information and an estimate of the damage that its disclosure could have, either in terms of the financial cost or the potential damage to the organisation's reputation.
The appropriate classifications are detailed in the Information Classification policy.

Intellectual Property Rights

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

Business Continuity and Disaster Recovery Plans

Information owners shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

ITS shall ensure that systems recovery plans are aligned with the business impact assessment to ensure that systems are recovered in order of priority.

Exchange of information

Data sharing agreements, procedures and controls will be established for enabling appropriate exchange of information, whilst maintaining compliance with relevant legislations, such as the Data Protection Act 1998.

Technical measures, such as encryption, should be proportionate to the classification of the information being processed.

Further details on information classification are available in the Information Classification policy.

Third party suppliers must comply with these procedures.

Reporting

The Assurance Manager and IT Security Manager shall keep the Information Governance Group informed of the information security status of the organisation by means of regular reports and presentations.

5.2. Information Technology

Computer Access Control / Authorisation

Access to IT facilities shall be restricted to authorised users who have business need to use the facilities,. Users who require access must sign the 'IT Computer System Fair Use Policy' before access is granted

Access to information systems should be authorized by immediate superiors in accordance with the system owner directives. This includes access rights, including accompanying privileges. Authorizations should only be granted on a "need to know" basis, and regulated according to role

Roles and responsibilities with accompanying access rights should be described based on the following classifications.

- Internal (several roles)
- External (several roles)
- Student
- Public
- Others.

Access to restricted areas such as Computer Rooms and Data Cabinets must be restricted to authorised IT and Contractor staff only. The development and maintenance of processes and procedures to record and monitor access is the responsibility of the IT Security Manager.

IT equipment classified as high risk or value must be protected against environmental threats (fires, flooding, temperature variations, etc.). Classification of equipment should be based on risk assessments.

Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier and appropriate business need.

Access rights will be amended following either a termination or change of employment.

Protection from Malicious Code

The organisation shall use software countermeasures and management procedures, under the direction of the IT Security Manager, to protect itself against the threat of malicious software and other system based vulnerabilities. All staff shall be expected to co-operate fully with this policy and associated guidance and procedural documents. Users shall not install software on the organisation's property without permission from the IT Security Manager. Users breaching this requirement may be subject to disciplinary action.

User Media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of IT Security Manager before they may be used on University of Sunderland's systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

The Removable Media Policy should be consulted for further information.

Mobile equipment and remote working

ITS provide systems to enable staff to work remotely in a secure manner.

Remote access to the University's network may only take place through security solutions approved by the IT Security Manager.

A policy on encryption controls will be developed with procedures to provide appropriate levels of protection to information whilst ensuring compliance with statutory, regulatory and contractual requirements.

Information classified as confidential or strictly confidential information and personal data shall only be taken for use away from the University in an encrypted form unless their confidentiality and security can otherwise be assured.

The confidentiality and security of information being transferred on portable media must be protected by use of approved corporate encryption techniques as defined by IT Security Standards.

Corporately provided Mobile units must be protected using adequate security measures. The use of Personal Mobile units for business use must be authorised by the IT Security Manager in all cases and must comply with the IT Security technical requirements before connection to the University's infrastructure is permitted.

Monitoring System Access and Use

Access and use of IT systems will be logged and monitored in order to detect unauthorized information processing activities.

ITS will register substantial disruptions and irregularities of system operations, along with potential causes of the errors.
ITS will log security incidents for all essential systems, involving the IT Security and Assurance Manager and invoking the University's Incident Response Plan as appropriate.

The University reserves the right record and monitor all IT activity within the computer systems and reserves the right to carry out security investigations where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act 1998.

Information Systems Acquisition, Development and Maintenance

The University shall ensure that all new information systems, applications and networks comply with technical and non technical security requirements and include a security plan which must be approved by IT Security and Business Assurance before they commence operation.

System Level Security Policies (SLSPs) will be developed by Information Asset Owners for systems under the organisation's control. Specific responsibilities will be assigned and obligations communicated directly to those who use the system.

Changes to information systems, applications or networks shall be reviewed and approved by the relevant Project and Change Management Board where appropriate, following consultation with the IT and Business Assurance team as appropriate.

Backup and Data Storage

The IT Department is responsible for carrying out regular backups and restores of data held in the corporate data stores in accordance with the Data Classification Matrix on Appendix A.

The use of local storage should be technically prohibited by the IT Department where possible and users should be discouraged from using local storage to manage their data requirements. Localyl stored data will fall outside of the IT Department remit of backup.

More Information can be found in the Backup And Data Storage Policy

Network Administration

The IT Department has the overall responsibility for the University's internal Network.

The IT department is responsible for ensuring that network access is granted in accordance with access policy. Users should only have access to the services they are authorized for. The access to privileged accounts and sensitive areas should be restricted. Users should be prevented from accessing unauthorized information.

There should be an automated inventory of all equipment connected to the wired and wireless network with measures implemented to ensure only approved and authorised equipment is permitted to connect.

Mobile units should be protected using adequate security measures. The use of Personal Mobile units for business use must be authorised by the IT Security Manager in all cases and must comply with the IT Security technical requirements before connection to the University's infrastructure is permitted.

Remote access to the University's computer equipment and services is only permitted if the security policy has been read and understood and the IT regulations signed.

More information can be found in the Network Access Policy
Metrics and Reporting

The IT Security Manager is responsible for ensuring that security metrics from all security based systems are recorded and reported at regular intervals to ITS and the Information Governance Group in order to provide confidence that security is under constant management and within acceptable tolerances. Systems and services that fall out of tolerances will be reported and remediated against under the supervision of the IT Security Manager.

6. RELATED POLICIES

This policy should be read in conjunction with the policies listed in Appendix A of the Overarching Information Governance Policy.