Newcastle University
Information Security Procedures
Version 3

A Information Security Procedures

Introduction

The University Information Security Policy addresses the information security of the University's information assets. These procedures provide detail on the principles addressed in the policy.

The Information Security Policy can be downloaded from www.ncl.ac.uk/iss/security/information-security-policy.doc

A-1 These Information Security Procedures provide management direction and support for Information Security across the University and as such shall be considered part of the University's Information Security Policy and shall have equal standing.

A-2 These Procedures have been prepared by the Director of Information Systems and Services of the University and ratified by Executive Board. They form part of the University's policies and procedures. They are applicable to, and will be communicated to, staff, students and other relevant parties.

A-3 These Procedures will be reviewed and updated regularly and in the light of any relevant changes to the law, University policies or contractual obligations.

A-4 To determine the appropriate levels of information security measures applied to information systems, a process of risk assessment shall be carried out for each system to identify the probability and impact of information security violations.

A-5 In order to manage Information Security within the University an Information Security Committee will be established, chaired by the Director of Information Systems and Services. The objective of this group will be to ensure that there is clear direction and visible management support for information security initiatives. This group shall promote information security through appropriate commitment and adequate resourcing.

A-6 The responsibility for ensuring the protection of information assets and that specific information security processes are carried out shall lie with the Head of the Academic or Service Unit managing that information asset.

A-7 Information Systems and Services will provide specialist advice on Information Security throughout the University.

A-8 Information Systems and Services will establish and maintain appropriate contacts with other organisations, including but not limited to: law enforcement authorities; regulatory bodies; network and telecommunications operators in respect of its Information Security Policy.

A-9 The implementation of the Information Security Policy and these Information Security Procedures will be reviewed by the University Auditors and the Director of Information Systems and Services on a regular basis.

B Business Continuity

Introduction

The Business Continuity Management and Planning Procedures set out the procedures for assessing and addressing risks to business continuity and define the responsibilities for preparing and implementing Business Continuity Plans.

Usually there will be a number of information assets, each with different continuity requirements depending on the level of criticality to the institution. The risk assessment process to classify information assets will be part of the University's standard risk management process. Appropriate Business Continuity Plans for each information asset classification can then be produced.

B-1 The Business Continuity Manager will be responsible for the University's Business Continuity Planning, liaising with the Director of Information Systems and Services and any relevant Service / Academic Unit Business Continuity Managers.

B-2 The Business Continuity Manager will monitor compliance with, and the effectiveness of these procedures on a regular basis.

B-3 A formal risk assessment exercise will be conducted to classify all information assets according to their level of criticality to the University and to determine where business continuity planning is needed. The risk assessment exercise will identify for each information asset the probability and impact of information security failures

B-4 A Business Continuity Plan will be developed for each relevant information asset. The nature of the plan and the actions it contains will be commensurate with the critically of the information asset to which it relates.

B-5 The Business Continuity Manager will ensure all business continuity plans are periodically tested. The frequency of testing will be as defined for the appropriate criticality level and will include tests to verify whether relevant management and staff are able to put the plan into operation.

B-6 The Business Continuity Plan will be communicated with all relevant staff. These persons will receive appropriate training to be able to carry out their roles with respect to the Business Continuity Plan.

B-7 The Business Continuity Manager will ensure each Business Continuity Plan will be periodically reviewed, and if necessary updated. The frequency of reviews will be as defined for the appropriate criticality level.

C Compliance

Introduction

The University Information Security Policy states that

> "The University will protect and manage its information assets to enable it to meet its contractual, legislative, privacy and ethical responsibilities."

The following procedures are to be referenced to ensure compliance with this statement.

C-1 Employee Conditions of Service and the University Statutes set out employees' responsibilities with respect to their use of information assets. Line managers will provide specific guidance on legal compliance to any member of staff whose duties require such guidance.

C-2 The Student Rules and Regulations incorporating the ISS Rules for Use of Computing Facilities set out all students' responsibilities with respect to their use of information assets.

C-3 All members of the University will comply with the Information Security Policy.

C-4 The University records retention policy defines the appropriate length of time for different types of record to be held. Records will not be destroyed prior to the expiry of the relevant retention period and will not be retained beyond that period (unless there is a requirement to do so under UK law). During the retention period appropriate technical systems will be maintained to ensure that the data can be accessed.

C-5 The University's information assets may sometimes be required for use as evidence. Where this is necessary, information shall be collected and presented to conform to the relevant rules of evidence. Expert guidance will normally be sought.

C-6 All University Information Assets will be operated and administered in accordance with the documented procedures. Regular compliance checks will be carried out.

D Outsourcing and Third Party Access

Introduction

The Outsourcing and Third Party Access Procedures set out the contractual conditions that are required to maintain the information security of the University's information assets when third parties are involved in their operation. This may occur in at least three distinct circumstances.

- When third parties are involved in the design, development or operation of the University's information assets. The University's data protection obligations apply irrespective of who is actually carrying out the processing.
- When access is granted to the University's information assets to third parties at remote locations where computer and network facilities may not be under the control of the University (this is covered in more detail by the Mobile Computing Procedures)
- When users who are not members of the University are given access to University information assets.

Each of these circumstances involves a risk to the University's information assets, which should be addressed before third party access is granted. Such access must be subject to appropriate contractual conditions and controls to ensure the risk can be managed.

D-1 All University information assets will be operated and administered in accordance with their documented procedures. Regular checks will be carried out to verify compliance. All third parties contracted to supply services to the University (or Unit within the University) must agree to follow the University's Information Security Policy.

D-2 Where appropriate, the University's Information Security Policy will be provided to any third party prior to any supply of services. Where deemed appropriate, the University will require the third party to sign a non disclosure agreement to protect its information assets.

D-3 Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of the University's Information Security Policy.

D-4 Any Third Party must ensure that any access to a University information asset is only to relevant authorised personnel and for the agreed purposes.

D-5 Any Third Party access to a University information asset will follow specific access methods as required at the time by the University.

D-6 Persons responsible for granting Third Party access to a University information asset will use reputable companies that operate in accordance with appropriate quality standards.

E Personnel

Introduction

The Personnel Procedures set out the process and responsibilities that are necessary to ensure that all members of the University contribute to the information security of its information assets.

Depending upon their role in the University, different individuals will have different levels of responsibility for information security, but in all cases these responsibilities need to be defined and individuals given appropriate training and support to enable them to fulfil their responsibilities.

E-1 All members of the University must comply with the Information Security Policy of the University. Any information security incidents resulting from non-compliance may result in action via the appropriate disciplinary procedure.

E-2 All members of the University should respect and protect the confidentiality of information assets, both during and after their membership of the University.

E-3 A non disclosure agreement will be used where necessary to protect the confidentiality, sensitivity or value of a University information asset.

E-4 Education and Training will be provided to raise information security awareness amongst members of the University.

E-5 Where a member of the University's access to information assets change, their information security needs will be reassessed and any new training or education provided as necessary.

E-6 Access to University information assets for a departing member of the University should be terminated promptly.

E-7 An employee who is disaffected may constitute a specific risk to the University's information assets. Upon notification that a member of the University has become disaffected, University management will consider whether the member's continued access to University information assets constitutes an unacceptable risk to the University and, if so, revoke relevant access rights. In any case where this action is being considered, the relevant manager will seek the advice of HR immediately.

F Operations

Introduction

The Operations Procedures set out how information assets will be managed and protected. It includes standard procedures for operation of key systems (including operation by end-user departments) and responsibilities of operators in normal conditions as well as fault and incident reporting and review. Processes for assignment of duties to staff that operate or use sensitive systems, should include consideration of whether segregation of duties is necessary. The Information Security Procedures also include rules for the migration of facilities from development to operational status.

F-1 Areas and offices where sensitive or critical information assets are processed will be given an appropriate level of physical security. Members of the University with authorisation to enter such areas will be provided with information on the potential information security risks and the measures used to control them.

F-2 The procedures for the operation and administration of the University's information assets must be documented. These documents will be regularly reviewed and maintained.

F-3 Duties and areas of responsibility will be segregated to reduce the risk and consequential impact of information security incidents.

F-4 Information Security Incidents as defined in the University's Information Security Policy will be reported via the Information Systems and Services Helpdesk.

F-5 Control procedures will be used to record changes to the operation and development of University's Information Assets.

F-6 Acceptance criteria for new information assets will be established and suitable tests of the information asset carried out prior to migration to operational status. Periods of parallel running will only be permitted where adequate controls, for the information security of the information asset and management of any live or test data, are in place.

F-7 The information security risks to all University information assets of system development projects will be assessed and access to those assets will be controlled.

F-8 Those who operate and administer the University's computers shall maintain a log of their activities. These operator logs will be subject to regular review.

F-9 Documentation, including distribution media or source program libraries, relevant to the information security of a University information asset will be protected from unauthorized access.

G Information Handling

Introduction

The Information Handling Procedures set out the need to define classes of University information assets and the requirements on the labelling, storage, transmission, processing and disposal of each class. Requirements may include confidentiality (in handling, storage and transmission), integrity (e.g. validation processes) and availability (e.g. backups). Confidential information assets will be subject to the rigorous treatment set out in this section; however, the principles should apply even to non-confidential information assets.

System documentation should itself be classified as sensitive information. This policy should be familiar to all staff dealing with information assets.

G-1 An inventory will be maintained of all the University's information assets and the ownership and classification of each asset will be clearly stated. Information assets will be clearly labelled and filed appropriately and according to classification.

G-2 When an information asset is to be disposed of, in line with retention periods, it will be irretrievably deleted, shredded or destroyed before the asset is moved off site, using procedures authorised by the owner of the Information Asset concerned.

G-3 When a third party is used to dispose of a University Information Asset, this should be done using procedures authorised by the owner of the Information Asset and in line with the University's Information Security Policy and Procedures and University Financial Procedures.

G-4 Information assets which contain sensitive data will undergo appropriate risk assessment, to determine if the asset should be destroyed, repaired or discarded. Such assets will remain the property of the University and may only be removed from site with the permission of the asset owner.

G-5 The University advocates a clear desk and screen policy. Screens on which confidential or sensitive information assets are processed will be sited so that they cannot be viewed by unauthorised persons wherever practicable.

G-6 Hard copies of confidential University information assets will be handled appropriately. Removal off site of confidential information assets will be authorised by an appropriate manager. Prior to authorisation, a risk assessment based on the criticality of the information asset will be carried out.

G-7 Information owners will ensure that appropriate backup, recovery and archival procedures are in place. The recovery processes, including from the archival medium, will be regularly tested. (Note – ISS can provide advice and support with this; in many cases, ISS can provide this service.)

G-8 The retention of information assets will take place with due consideration for legal, regulatory, business, administrative and historical values and in keeping with the University's Information Asset Retention Policy and/or Records Retention Policy.

G-9 Media used for the archiving of an information asset will be appropriate to the asset's expected longevity.

G-10 All users should handle University or Third Party Information Assets with due care and diligence.

G-11 Confidential University Information Assets will not rely on external information assets, which do not form part of the confidential asset concerned.

G-12 All signatures authorising access to, or release of, information assets will be properly authenticated.

G-13 Third parties in receipt of a confidential University Information Asset will maintain the confidentiality and integrity of that information asset. Relevant identity information for the Third Party will be verified prior to the dispatch of any information asset. The dispatch of the Information Asset will be authorised by the owner of the Information Asset concerned.

G-14 Confidential University Information Assets will only be transferred across information networks, when the confidentiality and integrity of those information assets can be assured.

G-15 Unsolicited or unexpected information assets will be handled with great care until the sender's identity has been verified, even if those assets have been received in error.

G-16 Transaction reports relating to a University Information Asset will be regularly reviewed by appropriate staff.

H. User Management

Introduction

The User Management Procedures set out how user accounts, privileges and access rights are managed.

H-1 Registration, deregistration and management of user access rights to University information assets is managed by Information Systems and Services. However, it is recognised that much of the control and operation of these processes will need to be handled locally, in schools or institutes. Such processes will be implemented across the University by suitably trained and authorised staff. A record of assigned user access rights will be maintained.

H-2 Alteration of access rights to University information assets, reflecting any change in business need or user role, will be done in a timely manner. User access right to any University information assets will be removed when a user leaves the University. Users' access rights will be reviewed at regular intervals. A record of altered user access rights will be maintained.

H-3 All users will have a unique identifier for their personal and sole use for access to University's information assets.

H-4 Password management procedures will be established to ensure the requirements of the Information Security Policy are fulfilled.

I Use of Computers

Introduction

The Use of Computers Procedures set out the responsibilities and behaviour of users with respect to University Information Assets.

I-1 University Information Assets will be secured appropriately - especially when left unattended.

I-2 Material downloaded from information networks will be treated with the utmost care to safeguard against both malicious and/or inappropriate content. Such material from unknown sources will only opened with good reason and should be scanned for possible malicious and/or inappropriate content.

I-3 University information assets and other essential information will be backed up regularly. It is the responsibility of the information owner to ensure that this takes place and the integrity of such backups is tested on a regular basis.

I-4 Care must be used when transporting University information assets to ensure that they are not lost, and that valid University information is not over-written by incorrect and/or out-of-date information.

I-5 Where a University information asset is encrypted, the encryption key will kept securely and not stored on the same asset that it protects.

I-6 Non-University owned equipment will only be connected onto the University data network with appropriate authorisation.

J Asset Planning

Introduction

The Asset Planning Procedures set out the criteria for the planning of new and/or updated University Information Assets. The installation and maintenance of information assets are covered in the Asset Management Procedures. Reference should be made to both of these procedures to ensure that planned assets will comply with information security requirements.

J-1 The procurement or development of new University information assets will be authorised appropriately by the University and comply with the University's Information Security Policy.

J-2 A risk assessment will be undertaken to identify the probability and impact of an information security failure in regard to any University information asset.

J-3 Equipment supporting the University's Information Assets will be planned with appropriate performance, robustness, reliability, accuracy, access rights and environmental protection.

J-4 Equipment supporting the University's Information Assets will be correctly maintained.

J-5 Prior to acceptance, all new or upgraded assets will be tested to ensure compliance with the University's Information Security Policy.

K Asset Management

Introduction

The Asset Management Procedures set out the responsibilities of those managing University Information Assets.

K-1 University's Information assets will be managed by suitably trained and qualified staff to oversee their day to day running and to preserve information security and integrity in collaboration with the owners of those assets. All information asset management staff will be given appropriate training.

K-2 Access to the University's information assets will use a secure log-on process. Passwords will be changed at frequencies which accord with best practice.

K-3 Access to the University's information assets may be limited by the location and suitable configuration of the initiating access request.

K-4 All access to the University's information assets will be logged and monitored to identify potential misuse of those assets.

K-5 Inactive connections to the University's Information Assets may be shut down after a defined period of inactivity to prevent access by unauthorised persons.

K-6 Operating system and/or other privileged access to University Information Assets will be restricted to those persons who are authorised to perform systems administration and/or management functions. Use of such access will be logged and monitored.

K-7 Changes to University Information Assets will be carefully planned and managed including the use of formal change control procedures and audit trails. All changes to assets will be properly tested and authorised before moving to the live environment.

K-8 Operational, information security event and error logs will be reviewed and managed by qualified staff on a regular basis.

K-9 IT System clocks must be regularly synchronised to suitably secured and authorative network time servers.

K-10 Vendor supplied modifications to University Information Assets will only be permitted under strictly controlled circumstances and with the authorisation of the owner of the relevant assets.

K-11 Up to date anti-virus and firewall techniques, and other controls as deemed necessary by information security staff, will be used to protect the integrity of the University's information assets. The management of these techniques and their licensing will be reviewed on a regular basis.

L Data Network Management – includes wireless networking

Introduction

The Network Management Procedures set out how the University's data networks are designed and assets are connected to them. It includes a requirement for continuing risk assessment and appropriate technical and procedural controls to reduce risk and to meet the requirements of the information handling procedures, as well as emergency measures to deal with faults and incidents.

Data networks should usually be partitioned to reflect different information security requirements, with control points preventing unnecessary traffic flows between and within partitions. Particular attention should be paid to protecting these control points from unauthorised access.

L-1 The University's data network will be managed by suitably authorised and qualified staff in Information Systems and Services, to oversee its day to day running and to preserve its information security and integrity in collaboration with individual asset owners. All data network management staff shall be given training as appropriate.

L-2 The data network must be designed and configured to deliver high performance and reliability to meet the University's needs, whilst providing a high degree of access control and a range of privilege restrictions.

L-3 The data network must be segregated into separate logical domains, with routing and access controls operating between the domains. Appropriately configured firewalls shall be used to protect the networks supporting the University's Information Assets.

L-4 Changes to network access points and/or connection of equipment to the University's data network will only be permitted in accordance with the relevant ISS regulations.

L-5 Local or remote access to the resources on the network will be strictly controlled. Access control procedures must provide adequate safeguards through robust identification, secure transmission and authentication techniques. Access to University Information Assets connected to the network will be strictly controlled.

L-6 Changes to the network will be carefully planned, authorised and managed. Formal change control procedures will be applied. All changes must be properly tested and authorised before moving to the live environment.

L-7 Data networks systems will be adequately configured and safeguarded against physical attack and/or unauthorised intrusion.

M Mobile Computing

Introduction

Modern computing and telecommunications devices make it increasingly easy to work when away from the office. Portable computing devices such as laptops, personal digital assistants (PDAs) and mobile phones can carry University Information Assets far from the University's premises and thereby expose them to different, and possibly increased, risks. The greatly increased availability of networked computers, from cybercafés to visitor facilities in other organisations, also encourages staff to access University Information Assets when away from the office. The University cannot rely on the information security integrity of such devices, nor on network connections having any information security controls. Therefore we must ensure that any University Information Assets that may be accessed remotely have sufficient inherent controls to protect them. Mobile computing of all kinds therefore raises significant issues for information security.

For some information assets it will be impracticable to provide adequate protection for access or storage by mobile computing. It is therefore likely and reasonable that the University will need to prevent some types of University Information Assets being used through mobile computing systems. In this, mobile computing differs from teleworking (covered in section N of this policy) where dedicated systems in a single, fixed location are used for access. By this definition, teleworking systems can be made as secure as office systems; mobile computing systems cannot.

It is likely that it is this area which will see the largest change in opportunity and threat in the coming years. Therefore, this section of the Procedures will need to be kept under frequent review.

M-1 The use of mobile devices to access University Information Assets will be authorised to do so by the appropriate information asset owner. A risk assessment based on the criticality of the information assets being used will be carried out.

M-2 The University will publish a set of guidelines for users of mobile computing equipment, advising them on how to use these devices in ways that conform to the University's Information Security Policy and other good practices.

N Teleworking

Introduction

It is increasingly common for some staff to spend part or all of their time working from a permanent remote location, often at home, using dedicated computer equipment. For the purposes of these procedures, this style of working is referred to as teleworking as opposed to mobile working which might involve the worker being in a number of different locations, or using shared or borrowed equipment. Teleworking raises additional information security issues beyond those of mobile working (see section M of these procedures) as teleworkers expect to have access to all the University Information Assets they would have in their office.

Computers used for teleworking are likely to have the same access to University Information Assets as internal computers, but without the protection provided by office walls, locked doors, data network controls and firewalls etc. Teleworkers may use the public internet to gain access to University Information Assets, so the privacy and integrity of information in transit must be assured.

N-1 A risk assessment based on the criticality of the information assets being accessed and the appropriateness of the proposed telework location will be carried out.

N-2 Teleworkers will be provided with appropriate computing and communications equipment and must only use this equipment for teleworking. The equipment provided may not be modified or replaced without suitable authorisation.

N-3 All teleworkers must use appropriate measures, based on a risk assessment, to protect the information security of information assets. Teleworkers must follow the agreed information security procedures at all times.

N-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

O Cryptography / Encryption of data

Introduction

The cryptography procedures set out when and how encryption will be used. It includes protection of sensitive information assets, key management, and procedures to ensure encrypted information can be recovered by the University if necessary.

At the date of issue, not all of the tools required to comply with this section of the Procedures are in place. Further, the point at which encryption takes place is not yet agreed. This will develop and the policy be updated through 2009.

O-1 Cryptographic controls will be developed to provide appropriate levels of protection to classified information assets whilst ensuring compliance with statutory, regulatory and contractual requirements.

O-2 Cryptographic controls will be established to ensure that authorized staff may gain access, when needed, to any University Information Asset held in encrypted form.

O-3 Confidential information will only be removed from the University in an encrypted form, unless specifically authorised.

O-4 The use of 'memory sticks' and data on CDs presents obvious risks. The confidentiality of University Information Assets transferred on portable media or across networks must be protected by the use of appropriate encryption techniques.

O-5 Encryption will be used for remote access connections to University Information Assets.

O-6 Cryptographic controls will be established for the management of electronic keys, to control both the encryption and decryption of sensitive information assets or digital signatures. These controls must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements.

O-7 Important University Information Assets being communicated electronically shall be authenticated by the use of digital signatures; information received without a valid digital signature shall not be relied upon.