

Introduction

What is information security and why do we need to think about it?

Information security is the practice of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so. It requires a range of skills and knowledge and increases in importance as our use of and reliance upon information grows.

All information has value. Sometimes this might be trivial but in many cases that value is substantial. Value can be measured in different ways, depending on the nature of information. In some cases, there may be a straightforward monetary value associated with given information. For others, emphasis is placed on different aspects of value. For example, the effects of unauthorised disclosure and loss of confidentiality.

The range of undesirable consequences associated with breaches of information security is long and includes:

- systems being unavailable;
- bad publicity and embarrassment;
- fraud;
- illegal personal investigation;
- industrial espionage.

How can information be protected?

Information security can be a daunting prospect for the average user. It is often seen as a highly technical discipline that requires expensive equipment and specialist assistance. While there are many situations that do need this type of approach, the most sensible and effective first steps are based on common sense and sound management practice.

Assessing and understanding the risks for our own organisation will help to establish appropriate risk management. In turn, this should ensure appropriate incident management and recovery when security is compromised.

For organisations of higher and further education a good level of information security can be achieved through the following:

- A pragmatic approach to policy and standards should be adopted resulting in an information security policy, which is supported by realistic and workable processes and procedures.
- The rigour of security measures applicable to any information system should be proportional to the assessed risk of the confidentiality, integrity or availability of its information becoming compromised.
- The risk assessment process should be light touch and might categorise the likelihood and consequences of any compromise of an information system's confidentiality, integrity or availability as being high, medium or low.
- Policies should not just be applicable to centralised IT services; the graduated model developed allows appropriate measures to be defined right down to individual PCs.
- A well informed, well trained workforce, who exercise an appropriate (but not excessive) level of vigilance, is an essential element of any security package.

What is the Information Security Toolkit and why is it needed?

There are a number of internal and external pressures facing universities and colleges which are driving the need for a more formal approach to information security, such as:

- an increased awareness of the need for proper security frameworks;
- an increased awareness of legal compliance requirements;
- the expansion of the role of auditors in organisational governance;
- the need to satisfy external bodies when working with sensitive data.

Across the whole community organisations are facing the same issues. The solution may be different for each but there are many common elements. This Information Security Toolkit provides step by step guidance and sample policies which organisations can combine and tailor to suit their own needs. It was developed by taking the control

guidelines contained in the British Standard BS 7799 as a starting point from which to derive a set of policies appropriate to higher and further education.

Throughout the Toolkit, references are made to BS 7799, the full reference being BS 7799–1:2005, *Information technology – Security techniques – Code of practice for information security management*. These should also be taken to be references to ISO/IEC 17799:2005, which has subsequently been adopted as ISO/IEC 27002. This is a standard code of practice which should be thought of as a comprehensive guide to good security practice. The second part of the standard, BS 7799–2:2005 (ISO/IEC 27001:2005) is a specification for an Information Security Management Systems (ISMS). An ISMS is the means by which senior management monitor and control their security. It forms part of an organisation’s internal control system. Guidelines for information security risk management can be found in part three of the standard, BS 7799–3:2006.

This edition 3 of the Toolkit replaces edition 2, which was based on an earlier version of the standards document that was published in 2000. A major change between the two versions of the standards was a renumbering of all of the controls. Additionally, most sections of the Toolkit have been updated to reflect a number of small changes in the contents of the standard.

What organisational policies are required?

The controls listed in BS 7799 can be grouped into policy documents about the organisation; about the use of information and information systems, and optional policies. The nature of each of these policies is set out in the table below. However, it is not essential that each of these policies exist as separate documents in every organisation. In many cases the information security requirements may already be covered by other more general policies, such as the Acceptable Use Policy (AUP).

Policies about the organisation

Information security	Top level document issued by senior management, stating the importance of information security to the organisation and the objectives and scope of the Policy. Defines responsibilities for information security and refers to more specific policy documents. Links to organisational contingency and disaster recovery plans. To be read by all users.
Business continuity planning	Documents that set out the process for assessing and addressing risks to business continuity. Defines responsibilities for preparing and implementing business continuity plans. To be read by those involved in business continuity planning.
Compliance	Document setting out how compliance with legal and other regulatory requirements is ensured. Likely to link to software management policy (for copyright/ licensing) as well as personnel and other policies. To be read by those responsible for compliance.
Outsourcing and third party access	Document setting out how any outsourcing or other access to or development of systems by third parties should be designed and managed to ensure information security. Includes initial risk assessment (which may conclude that an activity cannot safely be outsourced), contract terms, responsibilities, controls and reporting requirements. To be read by all those involved in outsourcing.
Personnel	Document setting out personnel procedures to ensure that the recruitment, management and departure of staff does not harm information security. Includes standard requirements and training for all posts plus identification of and appropriate resources for posts requiring additional checks and controls. Also includes responsibilities, terms and conditions, and disciplinary codes that all staff must agree to. To be read by all staff involved in personnel and management. Subsidiary documents will be read and agreed by all staff.

Policies about the use of information and information systems

Operations	Document setting out how information systems are operated to protect information security. Includes standard procedures for operation of key systems and responsibilities of operators in normal conditions as well as fault and incident reporting and review. Process for assignment of duties to staff should include consideration of whether segregation of duties is necessary. Also includes capacity management of information systems. To be read by all those involved in the design and operation of information systems.
Information handling	Document setting out the classes of information handled by the organisation and the requirements on the labelling, storage, transmission, processing and disposal of each. Requirements may include confidentiality (in handling, storage and transmission), integrity (e.g. validation processes) and availability (e.g. backups). System documentation should itself be classified as sensitive information. To be read by all staff dealing with information.
User management	Document setting out how user accounts and privileges are created, managed and deleted. Includes how new users are authorised and granted appropriate privileges as well as how these are reviewed and revoked when necessary, and appropriate controls to prevent users obtaining unauthorised privileges or access. Also includes recording of user activity on information systems and networks. To be read by all those responsible for authorising access to information systems or managing them.

Use of computers	Document setting out the responsibilities and required behaviour of users of information systems. Includes acceptable use, good practice in use of accounts and access credentials (e.g. passwords) and behaviour to protect against unknown or malicious code. To be read by all users.
System planning	Document setting out how information systems are designed, installed and maintained. Includes process for identifying requirements and risks, designing appropriately configured systems to meet them and assigning responsibility for their security. To be read by all those responsible for the design and deployment of information systems.
System management	Document setting out the responsibilities and required behaviour of those managing computer systems. Includes requirements on the maintenance and management of information systems and the software and services they run. Also required security software (e.g. antivirus) and configurations, as well as appropriate logging and monitoring of system activity, and expected behaviour when faults or incidents are detected. To be read by all those responsible for networked computers.
Network management	Document setting out how networks are designed and systems are connected to them. Includes continuing risk assessment and appropriate technical and procedural controls to reduce risk and to meet the requirements of the information handling policy, as well as emergency measures to deal with faults and incidents. Networks should usually be partitioned to reflect different 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. To be read by all those responsible for network management and connected systems.
Software management	Document setting out how software run on information systems is managed. Includes controls on the installation and use of software, the features provided and granting of access to software packages. Also includes maintenance of software with appropriate procedures for upgrades to minimise the risk to information. To be read by all those specifying or installing software.

Optional policies, required if these types of activity are planned

Mobile computing	Document setting out additional policies that apply to the use of portable computing devices and/or access from offsite locations. Includes process for authorizing such use and for determining additional measures necessary to combat the increased risk to information security that each represents. To be read by all those involved in designing, supporting or using mobile computing facilities.
Teleworking	Document setting out additional policies that apply to teleworking. Teleworkers are likely to require greater access to data and systems even than mobile workers so represent a greater security risk. Also includes procedures for maintenance and backup of teleworking systems and compliance with applicable regulations. To be read by all teleworkers and their managers.
Cryptography	Document setting out when and how encryption should (or should not) be used. Includes protection of sensitive information and communications, key management and procedures to ensure encrypted information can be recovered by the organisation if necessary. To be read by all users of encryption.