

How to use the *UCISA Information Security Toolkit*

The *UCISA Information Security Toolkit* has been constructed as an aid to organisations wishing to put in place a basic information security policy framework. This Toolkit can be used to develop organisational policies which can then be implemented over a period of time. Whilst it is possible to simply use the suggested policy statements in the Toolkit, it is strongly recommended that consideration is given to what would be the most appropriate policy for your own organisation. It is also important to remember that a policy alone will not improve your information security; the policy must also be implemented for its benefits to be realised.

The information security topics

The Toolkit is arranged in sections, each one covering an information security topic. These topics are defined by their intended audience, whereas BS 7799 divided its control areas by structures and processes. The first part of each section gives the definition of the topics addressed, according to the BS 7799 guidelines document, along with the relevant controls.

In every section, following the definition, a subsection maps the relationship between the suggested policies in this Toolkit and the related BS 7799 control references.

Guidelines for use

Within the *Guidelines for use* subsection, each topic is addressed with a short introduction followed by guidance on how to use the Toolkit to develop your own policy. This is followed by the Toolkit policy subsections that comprise a suggested policy statement, explanatory notes about that statement and information security issues that should be considered when implementing the policy. The policy subsections may also contain further information relevant to developing the policy.

Policy statements by criticality classification matrices

The final subsection for each topic contains a number of suggested policy statements which may constitute appropriate policies within that topic. Often, different statements are suggested for systems that have been assessed to have a low, medium and high degree of system criticality.

Example policies and policy statements

Each topic section is followed by example policies and/or policy statements included within that chapter. UCISA recommends that this section is used as a reference guide rather than the basis of an information security strategy. It is essential that the full context of each policy is understood and considered before inclusion in an organisation's strategy.

Information security management strategy

The purpose of information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. Information security management enables information to be shared, while ensuring the protection of information and assets.

Information takes many forms. It can be stored on computers, transmitted across networks, printed out or written down on paper, and spoken in conversations. From a security perspective appropriate protection should be applied to all forms of information, including papers, databases, films, view foils, models, tapes, diskettes, conversations and any other methods used to convey knowledge and ideas. The organisation's information and the IT systems and networks that it supports are important business assets. Their availability, integrity and confidentiality are essential to maintain efficient operations, value for money, legal compliance and a respected image.

The organisation is facing increasing security threats from a wide range of sources. Systems and networks may be the target of serious threats, including computer based fraud, espionage, vandalism and other sources of failure or disaster. New sources of damage, such as the highly publicised threats of computer viruses and computer hackers continue to emerge. Such threats to information security are expected to become more widespread, more ambitious and increasingly sophisticated. At the same time, because of increasing dependence on IT systems and services, the organisation is becoming more vulnerable to security threats. The growth of networking presents new opportunities for unauthorised access to computer systems and reduces the scope for central, specialised control of IT facilities.

In addition, legislation has been introduced, including the Data Protection Act 1998, the Copyright, Designs and Patent Act 1988, The Regulation of Investigatory Powers Act (RIPA) 2000 and the Computer Misuse Act 1990, that

place legal requirements on businesses to protect personal privacy and to ensure the confidentiality and security of their information. Holders of personal data must not only be registered under the Data Protection Act, but also take adequate steps to protect that data from unauthorised access.

The first stage in providing the organisation with adequate information security is the formulation of an information security policy, guidelines for its implementation and the appointment of an Information Security Officer.

The Information Security Policy

It is vital that this policy is comprehensive enough to cover all areas and concise enough to be understood. Specific security requirements can then be derived from the policy. If the policy is lacking in clarity then this provides a loophole for transgressors to use so it is, therefore, vital that a great deal of attention is paid to policy formulation. The policy, if constructed correctly, should allow the organisation to implement security procedures quickly and effectively.

Enforcement and penalties

The Information Security Policy and other related policies should be enforced by a combination of automated monitoring and network defence tools. These should be combined as necessary with direct audit and personal monitoring of systems and the use of agreed log files for reporting the outcome of routine tasks and tests. The results should be subject to scrutiny by the information security management team who should in turn report their findings to senior management.

In the event that an employee is aware of a potential breach of this policy, they should be encouraged to report their concerns to their manager. All such information should be treated in confidence. Any breaches of policy should be investigated, in conjunction with the HR Department, and appropriate penalties determined according to circumstances. Depending on the severity of the breach, penalties up to and including termination may be considered appropriate.

The review process

It should be the responsibility of the Information Security Officer and the information security management team to review the Information Security Policy on an annual basis.