



INFORMATION SECURITY POLICY

POLICY

Departments should ensure that adequate information security management policies are implemented to protect their information asset.

BACKGROUND

A department's information security plan should be formulated for dealing with risks and potential threats to their information asset in a manner commensurate with the department's business priorities, principles and goals. Security functionality should generally strike a balance between ease of use, relative cost, feasibility and availability of resources.

IMPLEMENTATION GUIDELINES

These guidelines should be considered a minimum set of required information security measures. It would be expected that a department's documented information security policy and procedures would be more prescriptive and would address :

- clear delegation of responsibility for the security of information resources including IT&T security focal points
- a Register of Security Incidents should be maintained to enable departments to regularly review all information security incidents and identify commonalities to improve their approach to security.
- minimum security requirements in key areas (including virus protection)
- a sustained staff education program. Information security policies and procedures must be documented and

understood by all. A copy needs to be secured off-site

- statement of the possible penalties that may be applied if the policy is not followed
- information security and recovery systems need to be endorsed by the department's Information Steering Committee, and periodically tested to ensure that resilience is achievable and practised
- plans should be periodically revised to ensure they remain relevant and complete.

These guidelines are taken directly from the British Standard BS 7799:1995 - *Code of Practice for Information Security Management*. The Draft Australian Standard AS 95305 was adapted from the British Standard. **IT MANAGERS SHOULD PURCHASE THESE STANDARDS.** Guidelines based on a recognised standard will enable IT managers to consider taking advantage of any future development of the standard.

The full standard provides detailed explanation and implementation should not be contemplated without reference to the full standards, which may be purchased from -

Standards Australia
19 Raglan Street
South Melbourne 3205

Phone: 9693 3500
Fax: 9696 1319

A synopsis of the British Standard follows -

- 1 - Security Policy
- 2 - Security Organisation

- 3 - Assets Classification and Control
- 4 - Personnel Security
- 5 - Physical Environmental Security
- 6 - Computer and Network Management
- 7 - System Access Control
- 8 - Systems Development and Maintenance
- 9 - Business Continuity Planning
- 10 - Compliance

e.g., auditors, users and administrators working together to address the problem effectively.

Security of Third Party Access

Policy: Access to departmental IT facilities by (non-departmental) third parties should be controlled.

Objective: To maintain the security of organisational IT facilities and information assets accessed by third parties.

Statement: Where there is a business need for such third party access, a security risk analysis should be carried out to determine the security implications and control requirements. The controls should be agreed and defined in a contract with the third party.

Such third party access may involve other participants. Contracts conferring third party access should include allowance for designation of other eligible participants and conditions for their access.

It is recommended that the BS 7799 code of practice be used as a basis for such contracts.

SECTION 1 - SECURITY POLICY

Information Security

Policy: Top management should set a clear direction and demonstrate their support for and commitment to information security through the issue of an information security policy across the organisation.

Objective: To provide management direction and support for information security.

SECTION 2 - SECURITY ORGANISATION

Information Security Infrastructure

Policy: A management framework should be established to initiate and control the implementation of information security within the organisation.

Objective: To manage information security within the organisation.

Statement: Suitable management forums should be established to approve information security policy, to assign roles, and to coordinate the implementation of security across the organisation. If necessary, a source of specialist information security advice should be established and made available within the organisation.

Contacts with external security specialists should be developed to keep up with industrial trends, standards and assessments, and to establish suitable liaison points for dealing with security incidents. Multidisciplined approaches to information security should be encouraged,

SECTION 3 - ASSETS CLASSIFICATION AND CONTROL

Accountability for Assets

Policy: All major information assets should be accounted for and have a nominated owner.

Objective: To maintain appropriate protection of organisational assets.

Statement: Accountability for assets helps ensure that adequate security protection is maintained. Owners should be identified for major assets and assigned responsibility for the maintenance of appropriate security measures. Responsibility for implementing security measures may be delegated, though

accountability should remain with the nominated owner of the asset.

Information Classification

Policy: Security classifications should be used to indicate the need and priorities for security protection.

Objective: To ensure that information assets receive an appropriate level of protection.

Statement: Information has varying degrees of sensitivity and criticality. Some items may require an additional level of security protection or special handling. A security classification system should be used to define an appropriate set of security protection levels, and to communicate the need for special handling measures to users.

SECTION 4 - PERSONNEL SECURITY

Security in Job Definition & Resourcing

Policy: Security should be addressed at the recruitment stage, included in job descriptions and contracts, and monitored during an individual's employment.

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

Statement: Managers should ensure that job descriptions address all relevant security responsibilities. Potential recruits should be adequately screened especially for sensitive jobs. All employees and third party users of IT facilities should sign a confidentiality (non-disclosure) undertaking.

User Training

Policy: Users should be trained in security procedures and the correct use of IT facilities.

Objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work.

Statement: Users should also be formally authorised in writing of the scope of their access (rights and restrictions).

Responding to Incidents

Policy: Incidents affecting security should be reported through management channels as quickly as possible.

Objective: To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

Statement: All employees and contractors should be made aware of the procedure for reporting the different types of incident (security breach, threat, weakness or malfunction) that might have an impact on the security of organisational assets.

They should be required to report any observed or suspected incidents as quickly as possible to the correct focal point. The organisation should establish a formal disciplinary process for dealing with employees who commit security breaches.

SECTION 5 - PHYSICAL ENVIRONMENTAL SECURITY

Secure Areas

Policy: IT facilities supporting critical or sensitive business activities should be housed in secure areas.

Objective: To prevent unauthorised access, damage and interference of IT services.

Statement: Such facilities should also be physically protected from unauthorised access, damage and interference. They should be sited in secure areas, protected by a defined security perimeter, with appropriate entry controls and security barriers. A clear desk policy is recommended to reduce the risk of unauthorised access or damage to papers and media.

Equipment Security

Policy: Equipment should be physically protected from security threats and environmental hazards.

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

Statement: Protection of IT equipment (including that used off-site) is necessary in order both to reduce the risk of unauthorised access to data and to safeguard against loss or damage. Attention should also be given to equipment siting and disposal. Special measures may be required to protect against hazards or unauthorised access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

SECTION 6 - COMPUTER AND NETWORK MANAGEMENT

Operational Procedures and Responsibilities

Policy: Responsibilities and procedures for the management and operation of all computers and networks should be established.

Objective: To ensure the correct and secure operation of computer and network facilities.

Statement: This should be supported by appropriate operating instructions and incident response procedures. The principle of segregation of duties should be applied, where appropriate, to reduce the risk of negligent or deliberate system misuse.

System Planning and Acceptance

Policy: Advance planning and preparation are required to ensure the availability of adequate capacity and resources.

Objective: To minimise the risk of systems failures.

Statement: Projections of future capacity requirements should be made, to reduce the risk of system overload. The operational requirements of new systems should be established, documented and tested prior to their acceptance. Fallback requirements for services supporting multiple applications should be coordinated and regularly reviewed.

Protection from Malicious Software

Policy: Precautions are required to prevent and detect the introduction of malicious software.

Objective: To safeguard the integrity of software and data.

Statement: A range of malicious techniques has been developed to exploit the vulnerability of computer software to unauthorised or unknown modification, with names such as 'computer viruses', 'network worms', 'Trojan horses' and 'logic bombs'. Managers of IT facilities should be alert to the dangers of malicious software, and should, where appropriate, introduce special measures to prevent or detect the introduction of malicious software. In particular, it is essential that precautions are taken to prevent and detect computer viruses on personal computers.

Housekeeping

Policy: Housekeeping measures are required to maintain the integrity and availability of services.

Objective: To maintain the integrity and availability of IT services.

Statement: Routine procedures should be established for taking back-up copies of data, logging events and faults and, where appropriate, monitoring the equipment environment.

Network Management

Policy: The security management of computer networks, which may

span organisational boundaries, requires special attention.

Objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

Statement: Special measures may also be required to protect sensitive data passing over public networks.

Media Handling and Security

Policy: Computer media should be controlled and physically protected.

Objective: To prevent damage to assets and interruptions to business activities.

Statement: Appropriate operating procedures should be established to protect computer media (tapes, disks, cassettes), input/output data and system documentation from damage, theft and unauthorised access.

Data and Software Exchange

Policy: Exchanges of data and software between organisations should be controlled.

Objective: To prevent loss, modification or misuse of data.

Statement: Such exchanges should be carried out on the basis of formal agreements. Procedures and standards to protect media in transit should be established. Consideration should be given to the business and security implications associated with electronic data interchange (EDI) and electronic mail exchanges and to the requirements for security controls.

SECTION 7 - SYSTEM ACCESS CONTROL

Business Requirement for System Access

Policy: Access to computer services and data should be controlled on the basis of business requirements.

Objective: To control access to business information.

Statement: This should take account of policies for information dissemination and entitlement.

User Access Management

Policy: There should be formal procedures to control allocation of access rights to IT services.

Objective: To prevent unauthorised computer access.

Statement: The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access to IT services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights which allow users to override systems controls.

User Responsibilities

Policy: The cooperation of authorised users is essential for effective security.

Objective: To prevent unauthorised user access.

Statement: Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

Network Access Control

Policy: Connections to networks should be controlled.

Objective: Protection of network services.

Statement: This is necessary in order to ensure that connected users or computer services do not compromise the security of any other networked services. Controls should include the following:

- a) appropriate interfaces between networked services;

- b) appropriate authentication mechanisms for remote users and equipment; and
- c) control of user access to IT services.

Computer Access Control

Policy: Access to computer facilities should be controlled.

Objective: To prevent unauthorised computer access.

Statement: Such access should be restricted to authorised users. Computer facilities that serve multiple users should be capable of the following:

- a) identifying and verifying the identity, and if necessary the terminal or location of each authorised user;
- b) recording successful and unsuccessful system access;
- c) providing a password management system which ensures quality passwords; and
- d) where appropriate, restricting the connection times of users.

More powerful access control systems, such as challenge-response systems, are also available at higher cost, if these are justified on the basis of business risk.

Application Access Control

Policy: Logical access controls should be used to control access to application systems and data.

Objective: To prevent unauthorised access to information held in computer systems.

Statement: Logical access to computer software and data should be restricted to authorised users. Application systems should:

- a) control user access to data and application system functions, in accordance with a defined business access policy;

- b) provide protection from unauthorised access for any utility software that is capable of overriding system or application controls; and

- c) not compromise the security of other systems with which IT resources are shared.

Monitoring System Access and Use

Policy: Systems should be monitored to ensure conformity to access policy and standards.

Objective: To detect unauthorised activities.

Statement: This is necessary in order to determine the effectiveness of measures adopted and to ensure conformity to an access policy model.

SECTION 8 - SYSTEMS DEVELOPMENT AND MAINTENANCE

Security Requirements of Systems

Policy: Security requirements should be identified and agreed prior to the development of IT systems.

Objective: To ensure that security is built into IT systems.

Statement: Security countermeasures are substantially cheaper and more effective if incorporated in application systems at the requirements specification and design stages. All security requirements, including the need for fallback processing, should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

Security in Application Systems

Policy: Appropriate security controls, including audit trails, should be designed into application systems.

Objective: To prevent loss, modification or misuse of user data in application systems.

Statement: The design and operation of systems should conform to commonly accepted industry standards of good security practice, as defined in this code of practice.

Note: Attention is also drawn to relevant legislation and any contractual obligations.

Additional countermeasures may be required for systems that process, or have an impact on, exceptionally sensitive, valuable or critical organisational assets. Such measures should be determined on the basis of specialist security advice, taking account of identified security threats and their possible business impact.

Security of Application System Files

Policy: Access to system files should be controlled.

Objective: To ensure that IT projects and support activities are conducted in a secure manner.

Statement: Maintaining the integrity of applications systems should be the responsibility of the user function or development group to whom the application system or software belongs.

Security in Development and Support Environments

Policy: Project and support environments should be strictly controlled.

Objective: To maintain the security of application system software and data.

Statement: Managers who are responsible for application systems should also be responsible for the security of the project or support environment. they should ensure that all proposed system changes are reviewed to ensure that they do not compromise the security of either

the system or the operating environment.

SECTION 9 - BUSINESS CONTINUITY PLANNING

Aspects of Business Continuity Planning

Policy: Business continuity plans should be available to protect critical business processes from the effects of major failure or disasters.

Objective: To have plans available to counteract interruptions to business activities.

Statement: There should be a process to develop and maintain appropriate plans for the speedy restoration of critical business processes and services in the event of serious business interruptions. Such interruptions may be caused by, for example, natural disasters, accidents, equipment failures, deliberate action, loss of supplied services or loss of utilities.

Business continuity planning should include measures to identify and reduce risks, limit the consequences should a threat be realised, and ensure speedy resumption of essential operations.

SECTION 10 - COMPLIANCE

Compliance with Legal Requirements

Policy: The design, operation and use of IT systems may be subject to statutory and contractual security requirements.

Objective: To avoid breaches of any statutory, criminal or civil obligations and of any security requirements.

Statement: All relevant statutory and contractual requirements should be explicitly defined and documented for each IT system. The specific controls, countermeasures and individual responsibilities to meet these requirements should be similarly defined and documented.

Advice on specific legal requirements should be sought from the organisation's legal advisers.

Security Reviews of IT Systems

Policy: The security of IT systems should be regularly reviewed.

Objective: To ensure compliance of systems with organisational security policies and standards.

Statement: Such reviews should be done against the appropriate security policies, and the technical platforms and IT facilities checked for compliance with security implementation standards.

System Audit Considerations

Policy: There should be controls to safeguard operational systems and audit tools during system audits.

Objective: To minimise interference to/from the system audit process.

Statement: Security protection is also required to safeguard the integrity, and prevent misuse of, audit tools.

OTHER RELEVANT INFORMATION

Disciplinary Action

The extent of disciplinary action to be taken where a violation has occurred depends on a number of factors. These factors include the severity of the violation, the extent of the evidentiary material, the mechanisms utilised to achieve the breach, the nature of the data contained on the system being violated and finally whether the violation is perceived to have been made by a public sector officer. A prescriptive step by step course of action is therefore difficult to define. **The course of disciplinary action to be undertaken must be determined by the CEO (or delegate) on a case by case basis.**

The largest scope for recourse, is where both internal and external disciplinary measures are available. This is available where the violation

is believed to have been performed by a public sector officer. Where the violation is of an external nature, the department has less scope for recourse, namely only the external disciplinary processes.

Internal Disciplinary Processes

The process for addressing violations of an internal nature is reasonably well defined. The Public Sector Management Act 1992 and supporting regulations outlines breach of discipline processes.

The Code of Conduct for the Victorian Public Sector also documents how officers must act when utilising information.

External Disciplinary Processes - Reporting to Police

Independent of whether the violation is an internal or external matter, where it is considered a criminal offence, the Police (Federal and/or State) should be informed. **The decision to involve police must be determined by the Secretary or CEO (or delegate).**

In doing so it is necessary to ensure that any evidence is secured.

Victoria Police

The Victoria Police should be contacted for specific criminal offences, however the violation may become a Federal matter through the process defined below. Relevant legislation includes the Crimes (Computers) Act 1988 - Victoria and the Crimes Act 1914.

Australian Federal Police (AFP)

The AFP should be involved where :

- a telecommunications line from a carrier is utilised during a security violation to computing equipment and/or
- the violated computer is considered to be a Commonwealth computer.

It must be recognised that the need for the computer to be considered a Commonwealth computer is not as limiting as it would initially appear. The scope of this definition is very wide. A computer is considered a Commonwealth computer where the computer facilities are utilised to store information at the

direction or request of the Commonwealth Government (ie taxation information, information required under Commonwealth State agreements, etc) or simply in the course of performing a contract with the Commonwealth Government.

<http://www.dpc.vic.gov.au/ocmpol/216e.htm>

