Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197 Email: assist@dsd.gov.au

HANDBOOK 4

SECURITY MANAGEMENT

Version 1.0

Objectives

401.   The 'Standard' defines a comprehensive set of security controls. The purpose of this document is to detail clearly how the Australian Standard can be applied in Government. Please note that this handbook will not duplicate the information contained within the Standard. As such, users of this handbook will be required to obtain a copy of the Standard to fully understand the requirements.

Australian Standard on Information Security Management

402. The Standard defines security controls regardless of the operating environment of the systems. It has been drafted based on the British Standard BS7799:1995 "Code of Practice for Information Security Management". The Standard is divided into categories, each of which covers different aspects of security: Security Policy; Security Organisation; Access Classification and Control; Personnel Security; Physical and Environmental Security; Computer and Network Management; System Access Control; Systems Development and Maintenance; Business Continuity Planning; and Compliance. The controls are comprehensive, and it is highly unlikely that all the controls will apply to any given site or system. Judgement is therefore required not only as to whether security controls are applicable to a site, but also as to the degree or grade of countermeasure required in applying the controls. It is therefore strongly recommended that a risk assessment be undertaken ***before*** considering the security controls defined in the Standard.

403. Those persons or agencies applying the Standard to Government systems need to be mindful of the established security guidelines, authorised for use within Government. In particular, the Attorney-General's Department publishes the Protective Security Manual (PSM). This manual is the baseline security policy document for Federal Government agencies, and contains a wealth of information on issues relating to personnel, physical and information security. The PSM can be obtained by contacting the Attorney-General's Department through the link shown in the **Introduction**.

404. The Standard defines ten 'key controls' that are particularly important in security management. The ten key controls are listed and further explained in **Annex A** to this handbook. These controls should be used to establish a security baseline when undertaking security management or reviewing system security. The first key control is ensuring that an organisation has an Information Security Policy Document. Since this is the starting point for establishing a sound security management philosophy, guidance on the preparation of a security policy document is contained in **Annex B** to this handbook. Agencies are encouraged to draft the policy in their own terms and definitions, and in a manner acceptable to relevant agency management and staff.

Consistency with Government Security Policy Documents

405. Although the Standard is quite comprehensive in detailing the security issues that should be considered as part of system security implementation and management, there are other Government security documents that need to be considered in conjunction with the Standard. **Annex D** details those security controls that are addressed in some way either by the PSM, or by DSD documents including the Handbooks comprising ACSI 33.

406. The ACSI 33 has been drafted to be consistent with the PSM. The PSM remains the definitive Government security document. Users of the ACSI 33 are encouraged to contact DSD in event of any apparent conflict between publications.

407. A number of the security controls identified in the Standard, along with most of the PSM, raise the issue of security management being guided by a comprehensive risk assessment. Users of this and other security documents are strongly encouraged to consider the security risks to their organisation. The PSM deals with risk assessment and **Handbook 3 - Risk Management** provides a worked example, showing how risk assessment can provide better guidance to security management.

ANNEX A

THE TEN KEY CONTROLS

A1. The AS/NZS 4444:1999 defines a number of controls. DSD is highlighting ten 'key controls' that are particularly important in Government IT security management. Those staff planning for security management activities or undertaking reviews of systems or sites should use the ten key controls as a baseline. These key controls, including the reference clauses, are listed below. A brief explanation of the intent of each of the controls is also included as an aid.

a. **Information Security Policy Document** (**Clause 1.1.2**). This control is required to ensure the organisation is clear on the security objectives relevant to the agency, and that endorsement for the policy has been granted by executive management. Further guidance on developing an organisational IT security policy is contained in **Annex B** to this handbook.

b. **Allocation of Information Security Responsibilities** (**Clause 2.1.4**). Clear statements defining those staff or agencies responsible for security functions need to be agreed and promulgated.

c. **Information Security Education and Training** (**Clause 4.2.2**). One of the most important and effective security countermeasures is education and training of users and managers of the organisation's information infrastructure.

d. **Reporting of Security Incidents** (**Clause 4.3.2**). It is critical that security incidents be addressed in a timely and thorough manner. Thought should be given to how best to deal with security incidents in the organisation.

e. **Virus Controls** (**Clause 6.4.2**). An increase in virus types and infection methods over the years has resulted in an overall increase in the threat likelihood of an information infrastructure being infected with a virus. An organisation should therefore spend reasonable resources when addressing this problem.

f. **Business Continuity Planning Process** (**Clause 9.1.2**). The process to develop contingency plans needs to be dynamic and owned by the organisation. There should be clear responsibilities and processes for developing these plans.

g. **Control of Proprietary Software Copying** (**Clause 10.1.2**). There are clear legal restrictions on the use of copyrighted material, and these restrictions should be formally observed and promulgated by an organisation.

h. **Safeguarding of Organisational Records** (**Clause 10.1.3**). In all organisations, regardless of size, there are those records whose high levels of integrity, confidentiality and/or availability are critical to the operations of the organisation. It is therefore important that these records be safeguarded.

i. **Data Protection and Information Privacy Legislation** (**Clause 10.1.4**).

The organisation must operate within the requirements of the law, including any relevant data protection and privacy legislation.

j. **Compliance with Security Policy** (**Clause 10.2.2**). Regular review of compliance with security policy should also be considered as necessary for effective security management.

ANNEX B

SECURITY POLICY DOCUMENT

B1. The IT Security Policy Document needs to describe the philosophy by which the organisation's security is managed. "Broad sweeping" security statements are discouraged from inclusion in these policies. Agencies are encouraged to draft the policy in their own terms and definitions, and in a manner acceptable to relevant agency management and staff.

B2. The IT Security Policy needs to detail objectives for management of various security aspects of the organisation's systems. The results of the risk assessment should be used to prioritise or focus efforts on those countermeasures that are important in mitigating identified risks. For example, if it is noted that a risk associated with "loss of information" through lack of controls on magnetic media may be a problem, then particular emphasis can be placed on controlling media. A **clear link** between the risk assessment and the security policy needs to be established, so that the security policy objectives and their associated countermeasures correspond to the level of required risk. This provides a degree of accountability in ensuring the security countermeasures are being efficiently employed.

B3. The IT Security policy may be divided into the following components:

i. **Organisation**. Detail the relationships and responsibility(ies) for security in the organisation. Describe how security policy is formulated, with particular regard to which formal groups or staff or consultative process is required by the agency before endorsing the policy. Describe the relationship with outside agencies that have a responsibility for providing security advice and assistance (examples may include Privacy Commissioner, DSD, Attorney-General's). Describe the relationships (if any) with service providers or other agencies where cooperation on security matters is required, or refer to legal or other documents that detail these relationships. Describe those responsible for undertaking security reviews or audits of the information systems.

ii. **Risk Assessment**. Include a reference to the risk assessment that will form the basis for this security policy. If possible, include the risk assessment as an annex to the policy, or include a summary of the findings as an annex to the policy.

iii. **Access Control**. Detail the maximum classification of data that will be handled, or could be accessed by staff in the organisation's information systems. The classification scheme should be as per the definitions of the Protective Security Manual. This section should detail some objectives for controlling access to key information resources (ie the start of an 'access control matrix'). The major data owner(s) should also be identified, where appropriate.

iv. **Personnel Security** (relating to IT Security). Detail the requirement for staff security clearances, and how this will be achieved. If no formal security clearance is required, detail the policy for background checking of staff to ensure inappropriate staff are not employed in positions of trust. Provide policy direction on which staff/contractors/consultants/auditors are allowed to enter the organisation's premises, be given accounts on internal systems etc. Also of importance is a plan for which particular staff or appointments may be granted superuser or privileged access to specified systems. Privileged access is defined as access which may give the user the ability to change key system configurations, have access to audit or related information, or have access to data streams, files and accounts owned by other users. This section should also detail the responsibilities associated with the use of the organisation's systems and the requirements for ensuring that users are made aware of their responsibilities, and penalty or breach clauses.

v. **Physical Security**. Detail the physical security objectives including, but not limited to, waste disposal, guarding, physical security alarms and response times, physical locks and physical security structure of all relevant premises.

vi. **Network and Communications Security**. Detail how network connections to outside agencies and organisations are to be approved and managed. This section should detail the policy objectives for handling and storage of cryptographic keys, such as those used in software or hardware based encryption systems.

vii. **Equipment Maintenance and Disposal**. Detail the policy objectives for ensuring integrity of the system hardware and software, and that data confidentiality is maintained when equipment is replaced, decommissioned or serviced. Policy objectives should include whether uncleared staff are allowed to maintain equipment, and if so how this would be achieved. The handling, control and disposal of storage media are important components of the overall security policy.

viii.**Configuration and Change Control**. Detail the responsibilities for approving changes to systems, and the process by which these changes should be approved. Stakeholders in the change process should be defined.

ix. **Contingency Planning**. Detail the critical management objectives for a contingency plan. A clear link between the risk assessment and the contingency objectives need to be established, so that the contingency policy objectives correspond to the level of required risk. The policy should define an "incident" and an "outage", and the authority responsible for declaration of an incident or an outage. An incident may not necessarily directly lead to an outage, but may require judgement to be exercised by a responsible authority. Policy guidance on recovery time objectives for the various grades of outages may be appropriate. Some guidance on the testing regime objectives and reporting of status of backup systems may also be required. This section may include reference to an organisation's Business Continuity Plan.

x. **Incident Response**. Detail clear definitions on the types of incidents that are likely to be encountered, so that a documented plan can be derived to alert management to the expected response. Security objectives for real-time reporting should be detailed, and needs to include when and how executive management should become involved. Detail the authority(s) responsible for initiating an internal investigation and police investigation of an incident. Note that this will link with contingency provisions as well as the organisation's fraud control plan. It would also be useful to include the ***criteria*** by which the responsible authority(s) would initiate a formal or police investigation of an incident. This section should also detail which agencies or authorities should be informed in event of an investigation being undertaken. Specific reference to anti-virus measures and viral incident response from a policy viewpoint should be addressed in this section.

xi. **Intrusion Detection and Audit**. Detail the intrusion detection objectives, incorporating the requirement for managing and maintaining intrusion detection tools and techniques, and management and review of audit trails. There should be an association between the objectives of intrusion detection, and the objectives of the incident response component (see above).

xii. **Storage Media**. Detail the objectives for managing storage media containing classified data. This includes management of media for backup and recovery.

ANNEX C

SECURITY TRAINING

Objectives

C1. No security scheme will be successful unless it is supported by security-trained staff. The staff must be adequately trained so that they are both able to discharge their responsibilities and understand and support the requirements for undertaking the agreed duties. The objective of this handbook is to detail some options for security training of identified staff.

Senior Management

C2. In order for senior management to have an appreciation of computer security, its problems and possible solutions, the Attorney-General's Department and DSD sponsor seminars for SES officers both in Canberra and in the other capital cities. On request, Attorney-General's and DSD are also prepared to tailor talks and seminars to meet the needs of the SES-level staff at individual agencies. Additionally, DSD has prepared a practical demonstration of computer system vulnerabilities, for presentation to senior management. This demonstration is available on request by addressing a letter to:

Assistant Secretary, Information Security Group,

Locked Bag 5076

Kingston ACT 2604

IT Professionals and Agency Security Staff

C3. System administrators and security administrators will require specialist training in the security features of the system(s). Vendors of a system normally provide instruction in the form of formal courses or self-tuition manuals. Third party vendors also offer courses for the more widely used systems. Third party courses, however, may be thinly disguised sales pitches and managers need to be aware of this problem.

C4. Vendor user group meetings and special interest groups can provide invaluable opportunities for system administrators and security administrators to advance their knowledge, expertise and exposure to particular systems. Examples of these groups include the Australian UNIX Users Group (**AUUG**) or the PC Users Group (**PCUG**).

C5. The Attorney-General's Department, in collaboration with DSD, runs courses suitable for those implementing computer security in their agencies and for staff who are to train other computer professionals and the user body. The courses range from personnel security to physical and IT security. These courses are very useful for those agency staff with little or no security training or experience. The course details can be obtained through **Protective Security Training Centre web site**. They can be contacted on **02 6273 4046** or email **trainingcentre.pscc@ag.gov.au**

User Awareness and Training

C6. All staff who have any access to their agency's computer systems will require some form of training, to assist them to discharge their security responsibilities. This type of training or 'awareness' is one of the most powerful security countermeasures available to system managers and security administrators. This form of training is almost invariably conducted in-house.

C7. The degree and content of the training will vary depending on the policy objectives of the agency. Nevertheless, the following topics, while not exhaustive, should be used as a guide for in any custom-developed user security training and awareness packages:

i. Purpose of the training/awareness program.

ii. Agency security appointments and contacts.

iii. Contacts and action in event of a real or suspected security incident.

iv. Legitimate use of system accounts.

v. Access and control of system media.

vi. Destruction and sanitisation of media and hardcopy output.

vii. Security of system accounts (including sharing of passwords).

viii. Authorisation for applications, databases and/or data.

ix. Configuration Control.

x. Use of the Internet Web and email (both Internet and Intranet).

C8. As well as formal training, awareness can be raised through use of ongoing reminders eg:

i. logon banners

ii. system access forms

iii. Departmental bulletins/memorandums

ANNEX D

SECURITY CONTROLS ADDRESSED IN GOVERNMENT SECURITY DOCUMENTS

D1. The following is a list of those security controls in the AS/NZS 4444:1999 that are addressed in whole or in part by other Government security documents. These documents include the Protective Security Manual (PSM), the Handbooks of the ACSI 33, and other DSD Information Security documents. The security controls listed below have been divided into the sections in which they appear in the Standard, for ease of reference.

Section 2

Information Security Co-ordination (**Clause 4.1.2**), **Allocation of Information Security Responsibilities** (**Clause 4.1.3**) and **Specialist Information Security Advice** (**Clause 4.1.5**) are all addressed in Volume A of the PSM ("Protective Security Policy"). Whilst there is considerable leeway for agencies to structure their information security management capability, there are some minimum standards addressed in the PSM relating to the appointment of a Senior Executive, appointments of an Agency Security Adviser (ASA), and an Information Technology Security Adviser (ITSA). **Cooperation between organisations** (**Clause 4.1.6**) is defined in Volume A of the PSM ("Protective Security Policy"), and includes those agencies in the

Commonwealth Government that have identified roles in the provision of security policy, advice or assistance. **Security Conditions in Third Party Contracts** (**Clause 4.2.2**) are contained in Volume F of the PSM ("Security Framework for Competitive Tendering and Contracting (CTC)"), which describes in detail the Government requirements for dealing with tenders and contracts.

Section 3
Classification Labelling (**Clause 5.2.2**) discusses the use of labels to identify information that requires protection. The Government has a long-established method of identifying the confidentiality requirements of official information with the use of classification labels. This is detailed in Volume C of the PSM ("Information Security"). Unfortunately, there is no similar system for labelling the integrity or availability requirements of information or systems.

Section 4
Security in Job Descriptions (**Clause 6.1.1**) suggests that security roles and responsibilities be clearly stated in job descriptions. Volume D of the PSM ("Personnel Security") states that all employees must be made aware of the broad security environment and security issues specific to their own work area. Whilst directly relating to security being addressed in job descriptions, the requirements of the PSM go further by ensuring employees are made aware (in a proactive manner) of their responsibilities. **Personnel Screening** (**Clause 6.1.2**) is addressed in Volume D of the PSM ("Personnel Security"). This volume is very specific about the steps required for processing security clearances, including initial recruitment screening. Users not familiar with the handling of Government classified information should become aware of all the requirements of this PSM volume. The processing of a security clearance or an "entry check" also includes the subject being required to sign an undertaking that they are aware of their responsibilities, and the conditions under which the clearance is issued. This is consistent with the requirements of the **Confidentiality Agreement** (**Clause 6.1.3**). **Reporting of Security Incidents** (**Clause 6.3.1**) is covered in Volume G of the PSM ("Guidelines on Security Incidents and Investigations"). Some ideas on Information **Security Education and Training** (**Clause 6.2.1**) are provided in **Handbook 12 - Malicious Software**.

Section 5
Removal of Property (**Clause 7.3.2**) and **Security of Equipment Off-Premises** (**Clause 7.2.5**) issues are addressed, in part, by Volume H of the PSM ("Security Guidelines on Home-Based Work"). Note however, there will be instances where equipment may be required to be removed and/or stored off-site without it being part of home-based work activities, such as for maintenance purposes. Further guidance on removal of security classified information from agency premises is also contained in Volume C of the PSM ("Information Security"). **Physical Security Perimeter** (**Clause 7.1.1**), **Physical Entry Controls** (**Clause 7.1.2**), **Security of Data Centres and Computer Rooms** (**Clause 7.1.3**), **Isolated Delivery and Loading Areas** (**Clause 7.1.5**) and **Clear Desk Policy** (**Clause 7.3.1**) security controls are covered in Volume E of the PSM ("Physical Security") and **Handbook 14 - Physical Security**, which details those minimum standards required for

storage and control of Government information. This volume also contains guidelines on physical security planning, protection of staff and clients, emergency management and conference security. Further detailed guidance on the "clear desk policy" is contained in Volume C of the PSM "Information Security". Security of cabling as detailed in **Cabling Security** (**Clause 7.2.3**) is further described in **Handbook 5 - Emanations and Cabling Security**. Disposal of equipment and media, particularly those that have been contaminated with sensitive data is addressed in **Handbook 6 - Media Security**, and supersedes **Secure Disposal of Equipment** (**Clause 7.2.6**) and **Disposal Of Media** (**Clause 8.6.2**).

Section 6
Volume C of the PSM ("Information Security") details the requirements for the handling, including transmission, of classified information, as suggested in **Information Handling Procedures** (**Clause 8.6.3**) and **Security of Media in Transit** (**Clause 8.7.2**) of the Standard. Volume G of the PSM ("Guidelines on Security Incidents and Investigations") is quite specific on the requirement for reporting incidents, as well as the procedures for investigating those incidents, as discussed in **Incident Management Procedures** (**Clause 8.3.1**). **Handbook 8 - Network Security** discusses in detail those network security issues that are addressed in part by **Network Security Controls** (**Clause 8.5.1**). **Handbook 11 - Email Security** discusses in detail those issues that need to be considered as part of an email system deployment, and supplement those issues discussed in **Security of Electronic Mail** (**Clause 8.7.4**).

Section 7
Whilst the Standard discusses the need for a **Access Control Policy** (**Clause 9.1.1**) as well as regular **Review of User Access Rights** (**Clause 9.2.4**), these issues are dealt with from a planning and technical point of view in **Handbook 7 - System Access Control**. Some parts of **Network Access Controls** (**Paragraph 9.4**) are covered either in part or in whole by the **Gateway Certification Guide**, published by DSD. This guide details the security requirements for the interconnection of networks, particularly those Government systems connecting to the Internet. **Handbook 8 - Network Security** also discusses the issues surrounding **Sensitive System Isolation** (**Clause 9.6.2**), particularly as they relate to Government classified systems. Intrusion Detection is covered in **Handbook 13 - Intrusion Detection and Audit Analysis**, which in part includes **Event Logging** (**Clause 9.7.1**) and **Monitoring System Use** (**Clause 9.7.2**).

Section 8
Cryptography and encryption techniques in Government are discussed in detail in **Handbook 9 - Cryptographic Systems,** which covers **Data Encryption** (**Clause 10.3.2**) and **Message Authentication** (**Clause 10.2.3**).

Section 10
The **National Archives of Australia** is responsible, in part, for implementation of the requirements of the *Archives Act 1983*. This includes

ensuring Government records are appropriately stored and made available to the public. The requirements published by National Archives supersede those outlined in **Safeguarding of Organisational Records** (**Clause 12.1.3**).

D2. It is important that those responsible for managing or advising Information Security requirements in Government be cognisant of the requirements of Handbook 1 of the ACSI 33, which covers the minimum standards required for Government systems. Whilst the other handbooks discuss options for the deployment of various countermeasures, Handbook 1 brings everything together in specifying those minimum standards required for classified systems.