Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

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

HANDBOOK 7

SYSTEM ACCESS CONTROL

Version 1.0

Objectives

701. Access Control mechanisms on information systems may have some or all of the following objectives:

a. To protect the confidentiality of identified information by permitting access only to those users that have a need to know.

b. To protect the availability of the system by controlling access to critical system functions (such as shutdown functions).

c. To protect the integrity of information by permitting access only to those staff that have the training and/or authority to make identified system changes.

702. Whilst access controls include those physical controls (such as locks, guards, etc), this handbook focuses on the functionality and requirements for system or logical controls. Physical security controls are covered briefly in **Handbook 6 - Media Security**.

The "Access Control Matrix"

703. Access Control systems essentially bring together two distinct entities, namely a user (or group of users) and the system's available resources. These two separate entities can be considered to be the two distinct components of an "access control

matrix". Visually, a simple "access control matrix" can be depicted as shown in **Table 1** below.

	Drive "T"	***Printer***	***CDROM***	***Email***	***Web***
J. Smith	Yes	Yes	No	No	No
S. David	Yes	No	Yes	Yes	No
J. Doe	Yes	Yes	No	No	No
S. Law	No	No	Yes	Yes	No
K. Jones	Yes	Yes	No	No	No

Table 1: Simple Access Control Matrix

704. In **Table 1**, the top row identifies the available resources, whilst the left-hand column identifies each user. The "access control matrix" brings together the users and resources in such a way as to facilitate the management of their access requirements. In this example, this is simply a "Yes" or a "No", to signify "allowed/disallowed", "enabled/disabled" or "on/off". For example, the user "J. Doe" is disallowed access to File X, yet authorised to user E-mail. In most real life cases, the level of access won't be a simple yes/no, but rather will be a degree of access. For example, the level of access may be "read only" which obviously prevents the users from writing, deleting or executing the object. Alternatively, it may be "read/write" but not "execute".

705. Note that this handbook primarily refers tological access control. However, a similar methodology could be applied to develop a physical access control matrix.

706. The essence of a successful access control matrix lies in the preparation. Accordingly, the following steps should be considered:

> a. Establish, at a broad level, the groups of resources that share the same or similar security objectives. The similarity may be based on requirements for confidentiality, integrity or availability. The resources should include ALL system resources, whether they will be protected by the operating system or by other mechanisms. They should include files, directories, applications, databases, hosts, services, etc.
>
> b. Develop groupings of users, whilst still meeting the objectives of the broad access control matrix. The 'group owner' should be evident once the groupings are stabilised.
>
> c. If necessary, define resource naming standards based on the findings under subparagraphs a. and b. above, to facilitate the resource groupings.

d. Once the user and resource groupings have been established, decide on the degree of access. This will depend on the security mechanisms used to protect the resource. Examples of possible degrees of access are READ, WRITE, EXECUTE, TAKE OWNERSHIP, ACCESS CONTROL, DELETE, PURGE, FILE SCAN, MODIFY.

e. Decide on the degree of devolvement for security administration. This is a balance between central security control and group administration, and is discussed later in this handbook.

707. Once a draft access control matrix has been developed, it is essential to obtain management agreement on the access constraints that are planned. The success of the access control matrix will depend on the agreement, approval and support afforded by management. This will become more critical as the extent of the matrix increases to cover the entire agency's resources, and the security responsibilities in ensuring the access control matrix meets the agency requirements is devolved to identified group and data managers.

708. The following paragraphs discuss in greater detail the requirements for an access control matrix.

Users and Groups

709. In a well-developed access control matrix for a medium to large organisation, a matrix that details access rights for all individual users would be cumbersome and impractical. It is therefore prudent that users be 'grouped', so that they may be allowed access in much the same way as individual users, without having to detail the accesses for each user. In almost all commercial operating systems available today, there are a number of default groups already configured for use with the system. Some examples of this are the "EVERYONE" or "WORLD" groups that may include all users of the system, the "ADMINISTRATORS" group, members of which may be allowed access to all administrative functions. Most operating systems and larger applications include a functionality to define groups as required by the security objectives. Note that standards on password and general account management are covered by the Australian Standard on information security management, as detailed in **Handbook 4 - Security Management**.

710. It is important to consider in developing a grouping structure in an access control matrix that groups are usually those users with common security needs. In other words, users tend to be grouped into **functional** teams. This may directly equate with **organisational** teams, but system administrators should note that this is not always the case and functional and organisational groupings can be quite distinct. An access control matrix developed using functional groupings will be more likely to require less maintenance and provide tighter access control than one based on an organisational structure.

711. Each grouping of users should have a clearly defined "group manager". This manager would be responsible for defining which users should be allowed membership of each group. This group manager is also a key to ensuring the

ongoing integrity of the group membership. Whether the group membership is checked manually or automatically, the group manager is the crucial link in ensuring the group membership is accurate and up-to-date. Ideally, the "group manager" should be provided with the appropriate access and training to manage the group structure, so that responsibility for group management is exercised by the group manager, and not through the system administrator.

System Objects and Resources

712. The top row of **Table 1** shows those system resources that are available for allocation to users and groups. In a fashion similar to the relationship between users and groups, the system's resources can be grouped into like functions, or more specifically, groups that allow access to the same or similar data. This can either be direct access, such as access to data located in files or volumes, or indirectly, such as through applications or databases. To this end, all the resources or objects identified as requiring some degree of access control should be listed. This is regardless of whether the control for these resources will be applied by the operating system or the application.

713. The resource groupings should also have a "data owner" associated with them. As for the "group manager" discussed above, the "data owner" will not only be responsible for the initial identification of resources, but also the continued checking of the access control system where appropriate. These "data owner" responsibilities are sometimes undertaken by the system administrator, although a more efficient and effective method is, as for the "group manager" role discussed above, for this task to be exercised by the identified "data owner". The degree of devolvement however, is dependent on the organisation's security policy.

Developing the Matrix

714. Once the groupings and group manager, and the resources and the data owners have been identified, the next step is to consider the level of access to be granted. The level of access may simply be a "allowed/disallowed", "enabled/disabled" or "on/off". However, there is usually much more flexibility available in designing an access control matrix to specify the appropriate access level more finely. As mentioned previously, the degrees of access control could include READ, WRITE, EXECUTE, TAKE OWNERSHIP, ACCESS CONTROL, DELETE, PURGE, FILE SCAN, MODIFY. This will be largely dependent on the security system's features.

715. In another example demonstrating the tasks listed above, users have been grouped according to the applications they run, and the resources (files, programs, procedures, etc) they access. Groups of users have then been associated with groups of resources. Some hierarchical trends may emerge with groups of junior staff each being associated with a single group of resources, and groups of more senior staff requiring access to several applications and thus several groups of resources.

716 A subset of a developed access control matrix may look like that shown in **Table 2**:

	HRMS Application Data Owner = Personnel Mgr	"Payroll" Database Data Owner = Payroll Mgr	"Personnel" Drive Data Owner = Registry Mgr	"Forms" Database Data Owner = Registry Mgr
"Personnel" Group Group Manager = Personnel Mgr	WX	R	W	R
"Payroll" Group Group Manager = Payroll Mgr	RX	W	W	R
"Registry" Group Group Manager = Registry Mgr	N	N	R	W
"Archives" Group Group Manager = Personnel Mgr	N	N	F	F

Legend: R = read, W = write, RX = execute read only, WX = execute write, N = no access, F = full access

Table 2: Subset of Developed Access Control Matrix

Ongoing Maintenance

717. An organisation's access control matrix should never become a static document, and should be continually reviewed and improved to meet the changing needs of the organisation.A number of key implementation factors will increase the likelihood that the document remains current and relevant to the organisation. These are:

a. Devolution of the group membership to identified "group managers".

b. Devolution of resource access control to identified "data owners".

c. Full support and approval from senior management.

d. Linkage between Human Resource Management Systems and security administration functions to track staff movements.

718. An organisation may decide to develop several access control matrices based

on resource categories to assist the management. If this is the case consistent identifiers should be used.

DAC and MAC

719. Some system administrators or security personnel may be familiar with the term "Discretionary Access Control" (DAC). This term is used in some implementations of trusted or evaluated products. DAC is essentially the same as has been discussed thus far in this chapter, and the formal definition for DAC (as defined in the NCSC-TG-003) is:

> "***A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.***"

720. Mandatory Access Control (MAC) is imposed on the user, by comparing the security clearance of the user, with the security classification of the object to which the user is requesting access. MAC is associated with trusted systems. The implementation of MAC is in many ways simpler than that for DAC, although existing installations with many users and files would be faced with a large initial labour cost for entering the users' clearances and classifying the files. Implementation of MAC may be expected to have a major effect on the operational functionality and efficiency of a system. Before acquiring such systems, agencies are strongly advised to seek DSD advice and assistance.

Identification and Authentication

721. The key to effective access control is reliable identification or authentication of users. One element that contributes to the reliability of individual authentication is good password management practices. Based on the risk assessment, **Handbook 3 - Risk Management**, the organisation should define a password policy covering the following elements:

a. length

b. use of dictionary words, extended characters, numerics, mixed case

c. expiry periods

d. history

e. grace logins

f. number of failed attempts

g. issue and re-issue procedures

h. suspension

722. Passwords are susceptible to brute force or dictionary attacks, and passwords using a mixture of case/special characters have been shown to be harder to break. The important aspect to note is to base the requirements on the level of risk. If these requirements are too onerous, they are more likely to be written down or circumvented. Password policies should be stronger for privileged accounts. User awareness is essential to maintaining a good password practice.

723. In areas of high risk, stronger authentication may be required eg:

a. biometrics

b. one-time password generators

c. cryptographic tokens

d. smartcards

e. asymmetric keys and digital certificates

724. Stronger authentication relies on combining one or more of the following:

a. something you know eg. password/PIN

b. something you have eg. token

c. who you are eg. biometrics

725. A successful access control and account management system can attribute system actions to individuals and leave little doubt as to the origin of all commands.

Grades of Access Control Implementations

726. The following grades of access control implementations have been included to assist in determining the level of effort that should be allocated to such a task. They are not definitive, and when implementing system access control should be used as a guide only.

a. **Grade 0**

i. Only system default groups used.

ii. Data allowed to be stored anywhere on the system.

iii. Access allowed to be changed by any user.

b. **Grade 1**

i. Large user groupings (member list 50). Default groups not changed.

ii. Sensitive data allowed to be stored in identified volumes or hosts.

iii. Access allowed to be changed by Administrator only.

iv. Disable system default accounts eg. 'guest'.

v. Organisation Password policy implemented on systems

c. **Grade 2**

i. Fine user groupings (member list < 50). Those default groups and accounts not required by the system are removed, inactivated or strictly controlled.

ii. Sensitive data allowed to be stored in identified volumes or directories.

iii. Access allowed to be changed by Data Owner(s) only, or system administrators acting on behalf of the data owners.

iv. Organisation Password policy implemented on systems

d. **Grade 3**

i. Detailed user groupings or individuals (member list < 10) required for storage of sensitive data. Those default groups not required by the system are removed.

ii. Sensitive data and applications only allowed to be stored in identified directories, databases or applications.

iii. Access allowed to be changed by Data Owner(s) only, or system administrators acting on behalf of the data owners.

iv. Tools implemented to check agreed access matrix.

v. Organisation Password policy implemented on systems

e. **Grade 4**

i. Access control implemented using MAC.

ii. Supporting DAC mechanisms NOT to be allowed or activated on the system.

iii. Regular verification of user clearances to be undertaken.

iv. Stringent Password policy implemented on systems