Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

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

HANDBOOK 1

NON-NATIONAL SECURITY STANDARDS FOR ELECTRONIC INFORMATION

Version 1.0

Objectives

101. The objective of this handbook is to define the minimum standards which apply to the protection of Australian Government systems that process, store, or transmit non-nationally classified information up to and including the PROTECTED level. Although some standards are outlined for systems at the HIGHLY PROTECTED level, these systems must also comply with the ACSI 37. In addition, when selecting a product for use within the Australian Government, its suitability needs to be assessed. The DSD **Evaluated Products List (EPL)**, which is discussed in **Handbook 2 - Evaluated Products**, provides a listing of products that have been deemed appropriate for use within the Australian Government.

Minimum Standards

102. **Table 1** describes the minimum standards for systems processing non-national security classified Australian Government information. When determining the appropriate minimum standard required, it is important to consider the highest classification level of data stored, as this will determine the overall classification of the system. In interpreting the table, the following issues should be noted:

a. A risk assessment **(Handbook 3)** MUST be undertaken for all systems, including those deemed to be UNCLASSIFIED.

b. Standards marked "Subject to Risk Assessment" are obviously

dependent on the outcome of the risk assessment. There should be a clear linkage between the outcomes of the risk assessment and the defined grade in the handbook.

c. The remark "As per Handbook X" is included in those cases where the requirements in the relevant handbook must be followed as there is no defined grade.

d. "Consult DSD" indicates that there may be further information that needs to be considered by the system manager. DSD can provide advice tailored to the specific requirements of the situation.

HANDBOOK REFERENCE	UNCLASSIFIED	IN-CONFIDENCE	PROTECTED	HIGHLY PROTECTED
Risk Assessment	Undertaken	Undertaken	Undertaken	Undertaken
System Access Control	grade 1	grade 1	grade 2	grade 2
Malicious Software	grade 1	grade 1	grade 2	grade 3
Security Management	As per Handbook 4	As per Handbook 4	As per Handbook 4	As per Handbook 4
Cryptographic Systems	As per Handbook 9	As per Handbook 9	As per Handbook 9	As per Handbook 9
Evaluated Products	As per Handbook 2	As per Handbook 2	As per Handbook 2	As per Handbook 2
Network Security	1, as per Handbook 8, and as per Table 2 in Handbook 2	1, as per Handbook 8, and as per Table 2 in Handbook 2	1, as per Handbook 8, and as per Table 2 in Handbook 2	1, as per Handbook 8, and as per Table 2 in Handbook 2
Emanations and Cabling Security	Consult DSD	Consult DSD	Consult DSD	Consult DSD
Media Security	grade 1	grade 1	grade 2	grades 2/3
Intrusion Detection	Subject to Risk Assessment	Subject to Risk Assessment	Subject to Risk Assessment	Subject to Risk Assessment
Web Security	Subject to Risk Assessment	Subject to Risk Assessment	Subject to Risk Assessment	Subject to Risk Assessment
Email Security	Subject to Risk Assessment	Subject to Risk Assessment	Subject to Risk Assessment	Subject to Risk Assessment
Physical Security	grade 1	grade 1	grade 2	grade 3

Table 1: Minimum Standards

103. The standards outlined in **Table 1** aim at affording agencies with maximum flexibility in determining deployment countermeasures according to risk. However, as these are minimum standards only, DSD should be consulted to discuss particular implementations on a case-by-case basis.

Recommended Standards

104. Some of the objectives in **Table 1** are identified as being "Subject to Risk Assessment". **Table 2** expands upon these rows providing an indication of the minimum **recommended** standard, based on the classification level.

HANDBOOK REFERENCE	UNCLASSIFIED	IN-CONFIDENCE	PROTECTED	HIGHLY PROTECTED
Intrusion Detection	grade 2	grade 2	grade 2	grade 3
Web Security	grade 1	grade 2	grade 2	grade 2
Email Security	grade 1	grade 2	grade 2	grade 2

Table 2: Minimum Recommended Standards

105. As an example, if considering **Web Security** for a system rated as PROTECTED, the minimum recommendation is for grade 2, as described in **Handbook 10**. However, if a higher grade is indicated by the risk assessment, it takes precedence. Thus it is important to note that whereas the entries in **Table 1** prescribe minimum standards, those in **Table 2** offer additional guidance only. Security standards derived from a risk assessment which exceed the grades outlined in **Table 2** will always take precedence.