Annex A Table 1 Handling CONFIDENTIAL classified information

Compromise of CONFIDENTIAL information's confidentiality would be expected to cause ➔

Business Impact Level 3A – Significant damage to the national interest, organisations or individuals

Sub-impact categories	Significant damage is:
Impacts on national security	causing damage to national security.
Impacts on entity operations	a. causing a severe degradation in, or loss of, organisational capability to an extent and duration that the entity cannot perform one or more of its functions for an extended time b. resulting in major long-term harm to entity assets.
Australian financial and economic impacts	a. undermining the financial viability of, or causing substantial financial damage to, a number of major Australia-based or Australian-owned organisations or companies b. causing long-term damage to the Australian economy to an estimated total of $10 to $20 billion c. causing major, short-term damage to global trade or commerce, leading to short-term recession or hyperinflation in Australia.
Impacts on government policies	a. significantly disadvantaging Australia in international negotiations or strategy b. temporarily damaging the internal stability of Australia or friendly countries c. causing significant damage or disruption to diplomatic relations, including resulting in formal protest or retaliatory action.
Impacts on personal safety	endangering small groups of individuals – the compromise of information could lead to serious harm or potentially life threatening injuries to a small group of individuals
Impacts on crime prevention	causing major, long-term impairment to the ability to investigate serious offences, ie offences resulting in two or more years imprisonment.
Impacts on defence operations	causing damage to the operational effectiveness or security of Australian or allied forces that could result in risk to life.
Impacts on intelligence operations	causing damage to Australian or allied intelligence capability.
Impacts on national infrastructure	damaging or disrupting significant national infrastructure.

Handling protections

Limiting dissemination of CONFIDENTIAL classified information

Need-to-know principle and dissemination/access restrictions:
a. security clearance to Negative Vetting 1 or above and need-to-know.

Records of dissemination – Classified Document Register:
a. it is good security practice to keep a record of incoming and outgoing information
b. it is good security practice to implement spot checks of information at this level.

How to transmit or transfer CONFIDENTIAL classified information, or remove it from an entity facility

Protect information when taken out of the office, for example for meetings:
a. in personal custody of individual and kept in a security briefcase or SCEC-approved pouch
b. subject to local entity arrangements for managerial approval.

Storage of information for home-based work prohibited unless home achieves all PSPF core requirements.

Protect information when transferred over public network infrastructure or through unsecured spaces. Encryption required for transfer over public networks or through Zone One security areas.

Protect information from unauthorised viewing when transferred within a single physical location, eg within an office:
a. single opaque envelope indicating the classification, receipt at discretion of originator, and either:
   i. passed by hand between people who have the appropriate security clearance and need-to-know or
   ii. placed in an approved satchel or pouch and delivered direct, by hand, by an authorised messenger
b. may be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between people with the appropriate clearance and need-to-know and there is no opportunity for any unauthorised person to view the information.

Protected information when transferred between physical establishments within Australia:
a. single opaque envelope that does not give any indication of the classification and placed in an approved satchel or pouch and delivered direct, by hand, by an authorised messenger and receipt required or
b. double enveloping and receipt required, and delivered by SCEC-endorsed courier.

Protect information when transferred between physical establishments outside Australia:
a. double enveloping required, receipt required and carriage by DFAT courier service or other authorised officers required.

How to use and store CONFIDENTIAL classified information

a. When information is unattended, protect it with a clear desk (for papers and removable storage media) and a clear screen for information processing facilities.
a. Protect information when stored or used as follows.

Protect information when stored or used in:	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
Storage	not permitted	SCEC Class B	SCEC Class C	SCEC Class C recommended	determined by entity risk assessment
Use	permitted	permitted	permitted	permitted	permitted

How to destroy and discard CONFIDENTIAL classified information

Paper waste:
a. only entity-assessed and approved or NAID AAA certified destruction service with specific endorsement and approved equipment and systems are to be used
b. if accountable material, under supervision of two officers cleared to the appropriate level who supervises the removal of the material to the point of destruction, ensure that destruction is complete, and sign a destruction certificate.

ICT media and equipment undergo sanitisation or destruction in accordance with ISM.