Appendix 4. Minimum protections and handling of PROTECTED information

Business Impact Levels (BIL) 3	PROTECTED—damage to the national interest, organisations or individuals
Protective marking	Apply text-based protective marking **PROTECTED** to documents (including emails). It is recommended that text markings be in capitals, bold text, large fonts and distinctive colours (red preferred) and located at the centre top and centre bottom of each page. If text-based markings cannot be used, use colour-based markings. For PROTECTED a blue colour is recommended. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios. If marking paragraphs, it is recommended that PROTECTED is written in full or abbreviated to (P) and placed either in brackets at the start or end of the paragraph or in the margin adjacent to the first letter of the paragraph.
Access	The need-to-know principle applies to all PROTECTED information. Ongoing access to PROTECTED information requires a Baseline security clearance or above. Any temporary access must be supervised.
Use	PROTECTED information and mobile devices that process, store or communicate PROTECTED information can be used in Zones 1-5. **Outside entity facilities (including at home)** PROTECTED information and mobile devices that process, store or communicate PROTECTED information: a. For regular ongoing home-based work, apply entity procedures, which must include conducting a security risk assessment of the proposed work environment b. For occasional home-based work, apply entity procedures on need for a security assessment and exercise judgement to assess environmental risk c. For anywhere else outside entity facilities (for example private sector offices, café): i. use of physical PROTECTED information is **not recommended**, if required, apply entity procedures and exercise judgement to assess environmental risk ii. use of mobile device that process, store or communicate PROTECTED information: apply entity procedures and exercise judgement to assess environmental risk
Storage	**Do not** leave physical PROTECTED information unattended, store securely when unattended. Mobile devices that process, store or communicate PROTECTED information can be left unattended if in a secured state, subject to entity clear desk policy. When storing physical PROTECTED information: a. inside entity facilities (Zones 2-5 only): i. Zones 4-5, store in lockable container ii. Zones 2-3, store in Class C container b. outside entity facilities: i. for regular ongoing home-based work, install and store in a Class C or higher container ii. occasional home-based work, apply requirements for carrying outside entity facilities, and retain in personal custody (strongly preferred), or for brief absences

	from home, apply entity procedures and exercise judgement to assess environmental risk. When storing a mobile device that processes, stores or communicates PROTECTED information a. inside entity facilities (Zones 1-5): i. Zones 4-5: if in a secured state, **recommend** storing in lockable container; if in an unsecured state, store in lockable container ii. Zone 2-3: if in a secured state, **recommend** storing in lockable container; if in an unsecured state, store in Class C container iii. Zone 1: if in a secured state, store in Class C container, if unsecured state, store in a higher zone. b. outside entity facilities: i. for regular ongoing and occasional home-based work, apply entity procedures and exercise judgement to assess environment risk ii. if in a secured state, **recommend** store in in lockable container; if in an unsecured state, store in a Class C or higher container.
Carry	When carrying physical PROTECTED information **always retain it in personal custody** a. inside entity facilities: i. Zones 1-5, in an opaque envelope or folder that indicates classification b. outside entity facilities (including external meetings) and between entity facilities: i. place in a security briefcase, pouch or satchel ii. **recommend** using tamper-evident packaging if aggregate information increases risk. When carrying a mobile device that processes, stores or communicates PROTECTED information a. inside entity facilities: i. Zone 2-5, if in a secured or unsecured state, apply entity procedures ii. Zone 1, carry in secured state; if in an unsecured state, apply entity in procedures b. outside entity facilities (including external meetings) and between entity facilities: i. carry in a secured state; if in an unsecured state, carry inside a security briefcase, pouch or satchel and consider tamper-evident packaging.
Transfer	When transferring PROTECTED information a. inside entity facilities (Zones 1-5): transfer by hand or entity safe hand and apply requirements for carrying; can be uncovered if office environment presents low risk of unauthorised viewing b. to another officer in a different facility i. apply requirements for carrying outside entity facilities ii. transfer by hand, entity safe hand, safe hand courier rated BIL 4, or DFAT courier (if transfer by courier, use tamper evident packaging). Any transfer requires a receipt.
Transmit	When transmitting electronically communicate information over PROTECTED networks (or networks of higher classification). Encrypt PROTECTED information for any communication that is not over a PROTECTED network (or network of higher classification).
Official travel	**Travel in Australia** PROTECTED information can be taken to external meetings and on domestic travel. When travelling with PROTECTED information or a mobile device that processes, stores or communicates PROTECTED information: a. apply requirements for carrying outside entity facilities and any additional entity procedures

	b. for airline travel, retain as carry-on baggage; if airline requires to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim as soon as possible Leaving PROTECTED information, or a mobile device that processes, stores or communicates PROTECTED information, unattended while travelling is **not recommended**. For brief absences from a hotel room, apply entity procedures and exercise judgement to assess environmental risk. **Travel outside Australia** Travelling overseas with physical PROTECTED information is **not recommended**—seek DFAT advice on options to access information at destination. If travel with physical PROTECTED information is required or when travelling a mobile device that processes, stores or communicates PROTECTED information: a. apply requirements for carrying outside entity facilities and any additional entity procedures (entities can consult DFAT for assistance in establishing procedures) and consider country-specific travel advice b. for airline travel, retain as carry-on baggage and **do not travel** if the airline requires it to be checked at the gate. **Do not** leave PROTECTED information or device unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility.
Disposal	Dispose of PROTECTED information using a Class B shredder.