Appendix 3. Minimum protections and handling of SECRET information

Business Impact Levels (BIL) 4	SECRET—serious damage to national interest, organisations or individuals
Protective marking	Apply text-based protective marking **SECRET** 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 SECRET a salmon pink 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 SECRET is written in full or abbreviated to (S) 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 SECRET information. Ongoing access to SECRET information requires a Negative Vetting 1 security clearance or above. Any temporary access must be supervised.
Use	SECRET information and mobile devices that process, store or communicate SECRET information can be used in security Zones 2-5. **Outside entity facilities (including at home)** **Do not** use SECRET information and mobile device that processes, stores or communicates SECRET information for regular ongoing home-based work a. Occasional home-based work is **not recommended**, if required: i. obtain manager approval ii. apply entity procedures on need for a security assessment iii. exercise judgement to assess environment risk **Do not** use SECRET information and mobile device that processes, stores or communicates SECRET information anywhere else outside entity facilities (for example private sector offices, café).
Storage	**Do not** leave SECRET information or a mobile device that processes, stores or communicates SECRET information unattended. Store securely when unattended. When storing physical SECRET information: a. inside entity facilities (Zones 3-5 only): i. Zones 4-5, store in Class C container ii. Zone 3, store in Class B container. b. outside entity facilities: **not recommended**, if required for occasional home-based work (see use above): i. apply requirements for carrying outside entity facilities ii. retain in personal custody (strongly preferred), or for brief absences from home, store in a Class B or higher container that has been approved as a proper place of custody by the Accountable Authority or their delegate iii. return to entity facility as soon as practicable. When storing a mobile device that processes, stores or communicates SECRET information:

	a. inside entity facilities (Zones 2-5 only): i. Zones 4-5: if in a secured or unsecured state, store in Class C container ii. Zone 3: if in a secured state, Class C container, if unsecured state, store in Class B container iii. Zone 2: if in a secured state, Class B container, if unsecured state, store in a higher zone. b. outside entity facilities **not recommended**, if required for occasional home-based work (see use above): i. apply requirements for carrying outside entity facilities ii. retain in personal custody (strongly preferred), or for brief absences from home, exercise judgement to store in a Class C or higher container that has been approved as a proper place of custody by the Accountable Authority or their delegate.
Carry	When carrying physical SECRET information **always retain it in personal custody** a. inside entity facilities: i. Zones 2-5, carry in an opaque envelope or folder that indicates classification ii. Zone 1, carry in an opaque envelope or folder that indicates classification and place in a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities: i. place in a security briefcase, pouch or satchel ii. **recommend** tamper-evident packaging if aggregate information increases risk When carrying a mobile device that processes, stores or communicates SECRET information **always retain it in personal custody** a. inside entity facilities: i. Zone 5, if in a secured or unsecured state, apply entity procedures ii. Zones 2-4, carry in secured state; if in an unsecured state, apply entity in procedures iii. Zone 1, carry in a secured state; if in an unsecured state, place inside a security briefcase, pouch or satchel. 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 seals.
Transfer	When transferring SECRET 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 very 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 over SECRET secure networks (or networks of higher classification). Use ASD's High Assurance Cryptographic Equipment to encrypt SECRET information for any communication that is not over a SECRET network (or network of higher classification).
Official travel	**Travel in Australia** Travelling domestically with SECRET information or with a mobile device that processes, stores or communicates SECRET information is **not recommended**. If required: 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 carry-on baggage to be checked at the gate,

	i. place in tamper-evident packaging within a security briefcase, pouch or satchel and try to observe entering and exiting the cargo hold and reclaim as soon as possible ii. if tamper-evident packaging not available, **do not travel**. **Do not** leave SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility. **Travel outside Australia** Travelling overseas with SECRET information, or with a mobile device that processes, stores or communicates SECRET information, is **not recommended**—seek DFAT advice on options to access information at destination. If travel with SECRET information or mobile device is required: a. apply requirements for carrying outside entity facilities and any additional entity procedures (entities can consult DFAT for assistance in establishing procedures), 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. If access to SECRET information or mobile device provided at destination: a. apply requirements for carrying outside entity facilities and any additional entity procedures b. retain in personal custody or store in an Australian entity facility. **Do not** leave SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility.
Disposal	Dispose of SECRET information using a Class A shredder.