Minimum protections and handling requirements for PROTECTED information

BIL 3	PROTECTED – serious damage to the state or national interest, organisations or individuals.
Protective marking	- Text-based marking **must** be applied to **PROTECTED** documents (including emails). - It is **recommended** that text markings are in capitals, bold, large fonts and a distinctive colour (red preferred). Markings **should** be placed at the top and bottom of each page. - If text-based markings cannot be used, colour-based markings **must** be used. The preferred colour for **PROTECTED** is blue (RGB 79, 129, 189). - For paragraph grading indicators, **PROTECTED** **should** be written in full or abbreviated to (P) and placed at the start or end of the paragraph or in the margin adjacent to the first letter.
Access	- Need-to-know principle applies to **all** **PROTECTED** information - Ongoing access to **PROTECTED** information requires a Baseline security clearance, or above. - Temporary access to **PROTECTED** information **must** be supervised.

Use	- **PROTECTED** can be used in security zones 1-5
	- Outside agency facilities (including at home):
	  ○ apply agency procedures which **must** include conducting a security risk assessment of the proposed work environment
	  ○ for occasional home-based use, apply agency procedures and exercise judgement to assess the environmental risk
	- Use of **PROTECTED** information outside agency facilities or the home (e.g. external agency offices, cafés) is **not recommended**, but if necessary:
	  ○ apply agency procedures and
	  ○ exercise judgement to assess the environmental risk

Storage	- **PROTECTED** information **must not** be left unattended. Information **must** be stored securely when unattended.
	Mobile devices that process, store or communicate **PROTECTED** information may be left unattended if in a secured state (password protected, encrypted etc.)
	- When storing **PROTECTED** information inside agency facilities (zones 2-5 only):
	  ○ in zones 4-5, store in a lockable container
	  ○ in zone 2-3, store in class C container
	- It is **not recommended** to store **PROTECTED** information outside agency facilities (including at home), but if necessary:
	  ○ apply requirements for carrying outside agency facilities
	  ○ for regular, ongoing home-based work, install and store in a Class C or higher container
	  ○ for occasional home-based work, retain in personal custody (positive control), or for brief absences from home, apply agency procedures and exercise judgement to assess environmental risk
	  ○ return to agency facilities as soon as practicable
	- When storing mobile devices which process, store or communicate **PROTECTED** information inside agency facilities (zones 1-5):
	  ○ in zones 4-5, if in a secured state, **recommended** storing in lockable container; if in an unsecured state, you **must** use a lockable container
	  ○ in zones 2-3, if in a secured state, **recommend** storing in a lockable container; if in an unsecured state, store in a Class C container
	  ○ in zone 1, if in a secured state, store in a Class C container; if in an unsecured state, store in a higher security zone
	- Storage of mobile devices outside of agency facilities:
	  ○ apply requirements for carrying outside agency facilities
	  ○ apply agency procedures and exercise judgement to assess environmental risk

	○ if in a secured state, **recommend** storage in a lockable container; if in an unsecured state, store in a Class C container or higher.
Carry	- When carrying **PROTECTED** information outside of agency facilities, information **must** be retained in personal custody (positive control) at all times. - Inside agency facilities: ○ in zones 1-5, in an opaque envelope or folder that indicates classification - Outside or between agency facilities, including for external meetings: ○ place in a security briefcase, pouch or satchel ○ **recommended** tamper-evident packaging - Mobile devices that process, store or communicate **PROTECTED** information: - Inside agency facilities: ○ in zone 2-5, if secured or unsecured, agency procedures are sufficient ○ in zones 1, carry in a secured state. If unsecured, apply agency procedures - outside or between agency facilities: ○ 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 inside agency facilities: ○ in zones 1-5, transfer by hand or agency safe-hand, and apply all necessary handling requirements. Can be uncovered if transfer is in close proximity and there is a low risk of unauthorised viewing - When transferring **PROTECTED** information outside agency facilities to another facility: ○ apply requirements for carrying outside agency facilities ○ transfer by hand, agency safe-hand, safe-hand courier rated to BIL 4, or DFAT courier (use tamper evident packaging). - A receipt of transfer **must** be obtained
Transmit	- Electronic transmission of unencrypted **PROTECTED** information **must** be over **PROTECTED** secure networks (or higher). Encrypt **PROTECTED** information for any communication that is not over a **PROTECTED** network (or higher).
Official travel	- **PROTECTED** information or mobile devices can be taken to external meetings and on domestic travel. - When travelling domestically with **PROTECTED** information (or mobile devices that process, store or communicated **PROTECTED** information): ○ Requirements for carrying outside agency facilities **must** be applied, including tamper-evident packaging ○ Information and/or device **should** be retained as carry-on baggage, but if not possible, try to observe entering and exiting the cargo hold and reclaim as soon as possible - **PROTECTED** information (or mobile devices) **should not** be left unattended while travelling domestically. For brief absences from a hotel room, apply agency procedures and exercise judgement to assess environmental risk - Travel outside of Australia with **PROTECTED** information is **not recommended,** but if necessary: ○ seek DFAT advice on options to access information or devices at overseas destination. ○ apply agency procedures for carrying outside agency facilities ○ Information and/or device **must** be retained as carry-on baggage, and travel **must not** occur, if airline requires baggage to be checked ○ **Do not** leave **PROTECTED** information or devices unattended. **Do not** store while travelling (e.g. hotel safe). If storage is required, store in an Australian agency facility.
Disposal	- **PROTECTED** information **must** be destroyed using a class B shredder.