Table 7 Minimum protections for information transmission and transfer

	OFFICIAL	Sensitive information OFFICIAL: Sensitive	Security classified information PROTECTED	SECRET	TOP SECRET
	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Protect information when taken out of the office, for example for meetings	✓ Information may be taken out of the office (in accordance with the person's duties), for example for meetings.	✓ Information may be taken out of the office (in accordance with the person's duties), for example for meetings.	✓ Information may be taken out of the office, for example for meetings. a. Secure information in personal custody in a security briefcase or SCEC-approved pouch.	✓ Information may be taken out of the office, for example for meetings, subject to local entity arrangements for managerial approval. a. Secure information in personal custody in a security briefcase or SCEC-approved pouch.	✓ Information may be taken out of the office, for example for meetings, but is not recommended. a. Written, manager-approved record of outgoing material maintained in an auditable log or CDR b. Secure information in personal custody in a security briefcase or SCEC-approved pouch.
Protect information when used for home-based work	✓ Information may be used for home-based work in accordance with the person's duties.	✓ Information may be used for home-based work in accordance with the person's duties. a. Secure information from unauthorised access.	✗ Not applicable. Storage of information for home-based work is prohibited unless home achieves all PSPF core requirements.	✗ Not applicable. Storage of information for home-based work is prohibited unless home achieves all PSPF core requirements.	✗ Not applicable. Use for home-based work is prohibited.
Protect information when transferred over public network infrastructure or through unsecured spaces	✓ Transfer over public network infrastructure or through unsecured spaces is permitted. a. Protect information in accordance with the person's duties.	✓ Encrypt information for transfer over public networks or through Zone One security areas. [Note i]	✓ Encrypt information for transfer over public networks or through Zone One security areas.	✓ Encrypt information for transfer over public networks or through Zone One security areas.	✓ High Assurance Cryptographic Equipment encryption required for transfer over public networks or outside Zone Five security areas.
Protect information from unauthorised viewing when transferred within a single physical location, eg within an office	✓ Transfer within a single physical location is permitted. a. Protect information in accordance with the person's duties.	✓ Transfer within a single physical location is permitted. a. Protect information in accordance with the person's duties.	✓ Transfer within a single physical location is permitted. a. Protect information in accordance with the person's duties.	✓ Transfer within a single physical location is permitted. a. Protect information in accordance with the person's duties.	✓ Transfer within a single physical location is permitted. a. Protect information in accordance with the person's duties.
Protect information when transferred between physical establishments within Australia	✓ Transfer between physical establishments within Australia is permitted. a. Protect information in accordance with the person's duties.	✓ Transfer between physical establishments within Australia is permitted if unauthorised access is deterred, eg external mail is sealed.	✓ Transfer between physical establishments within Australia is permitted if secured from unauthorised access. a. Double enveloping required if SCEC-endorsed courier used. b. Receipt required.	✓ Transfer between physical establishments within Australia is permitted if secured from unauthorised access. a. Double-enveloping and i. a security briefcase (or SCEC-approved pouch) and delivered direct by an authorised messenger[ii] or ii. SCEC-endorsed courier. b. Receipt required.	✓ Transfer between physical establishments within Australia is permitted if secured from unauthorised access. a. Double-enveloping and i. a security briefcase (or SCEC-approved pouch) and delivered direct by an authorised messenger[ii] or ii. safe hand courier. b. Receipt required.
Protect information when transferred between physical establishments outside Australia	✓ Transfer between physical establishments outside Australia is permitted. a. Protect information in accordance with the person's duties.	✓ Transfer between physical establishments outside Australia is permitted if unauthorised access deterred, eg external mail is sealed.	✓ Transfer between physical establishments outside Australia is permitted if secured from unauthorised access. a. Double enveloping b. Receipt required c. Carriage by DFAT courier service or an authorised officer[iii].	✓ Transfer between physical establishments outside Australia is permitted if secured from unauthorised access. a. Double enveloping b. Receipt required c. Carriage by DFAT courier service or an authorised officer[iii].	✓ Transfer between physical establishments outside Australia is permitted if secured from unauthorised access. a. Double enveloping b. Receipt required c. Carriage by DFAT courier service.

Table 1 notes:

[i] Encrypt OFFICIAL: Sensitive information transferred over public network infrastructure, or through un-secure spaces, unless the residual security risk of not doing so has been recognised and accepted by the entity.
An entity may also wish to consider other security measures or mitigating protections already in place, such as: validating the recipient's address before sending information in an unencrypted form; or sending sensitive information or large amounts of non-sensitive information as an encrypted or password protected attachment. Australian Privacy Principle 11 imposes additional obligations regarding the transmission of 'personal information' (as defined under the Privacy Act); the OAIC's Guide to Securing Personal Information provides guidance on the reasonable steps that entities may be required to take under the Privacy Act to protect the personal information they hold, including when such information is being transferred or transmitted.
ii An authorised messenger is an officer authorised in accordance with the entity's procedures to transfer sensitive and classified information that has been secured from unauthorised access, between physical establishments within or outside Australia. An authorised messenger does not require a security clearance appropriate to the level of sensitive or security classified information transferred.
iii An authorised officer is an officer authorised in accordance with the policies of the PSPF and the entity's procedures.