Minimum protections for information transmission and transfer

	Sensitive information		*Security classified information*		
Classification	**OFFICIAL**	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Business Impact Levels (BIL)	**1** **Low**	**2** **Low to medium**	**3** **High**	**4** **Extreme**	**5** **Catastrophic**
Protect information when taken out of the office for official purposes	✓ Yes, for official purposes	✓ Yes, for official purposes	✓ Yes, for official purposes, but: a. secure information in personal custody in a security briefcase or SCEC-approved pouch.	✓ Yes, for official purposes, but: a. subject to agency arrangements for managerial approval. b. Secure information in personal custody in a security briefcase or SCEC-approved pouch.	✓ Yes, 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	✓ Yes, for official purposes but a. In line with agency policies	✓ Yes, for official purposes but a. in line with agency policies b. 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	✓ Yes, for official purposes but a. NTK principle **should** be applied	✓ Yes, for official purposes but a. information **must** be encrypted for transfer over public networks or through Zone One security areas.[1]	✓ Yes, for official purposes but a. information **must** be encrypted for transfer over public networks or through Zone One security areas.[1]	✓ Yes, for official purposes but a. information **must** be encrypted for transfer over public networks or through Zone One security areas.[1]	✓Yes, for official purposes but a. **Must** use High Assurance Cryptographic Equipment encryption for transfer over public networks or outside Zone Five security areas.
Protect information when transferred within a single physical location (e.g. an office)	✓ Yes, for official purposes but a. NTK principle **should** be applied	✓ Yes, for official purposes but a. NTK principle **must** be applied	✓ Yes, for official purposes but a. NTK principle **must** be applied	✓ Yes, for official purposes but a. NTK principle **must** be applied	✓ Yes, for official purposes but a. NTK principle **must** be applied
Protect information from unauthorised access when transferred between physical establishments in Australia	✓ Yes, for official purposes but a. NTK principle **should** be applied	✓ Yes, for official purposes but a. unauthorised access **must** be deterred, e.g. external mail is sealed.	✓ Yes, for official purposes but a. **must** be secured from unauthorised access. b. Double enveloping required if SCEC-endorsed courier used. c. Receipt required.	✓ Yes, for official purposes but a. **must** be secured from unauthorised access. b. Double-enveloping and i. a security briefcase (or SCEC-approved pouch) and delivered direct by an authorised messenger[2] or i. SCEC-endorsed courier. c. Receipt required.	✓ Yes, for official purposes but a. **must** be secured from unauthorised access. b. Double-enveloping and i. a security briefcase (or SCEC-approved pouch) and delivered direct by an authorised messenger[2] or ii. safe hand courier. c. Receipt required.
Protect information from unauthorised access when transferred between physical establishments outside Australia	✓ Yes, for official purposes but a. NTK principle **should** be applied	✓ Yes, for official purposes but a. unauthorised access **must** be deterred, e.g. external mail is sealed.	✓ Yes, for official purposes but a. Double enveloping b. Receipt required c. Carriage by DFAT courier service or an authorised officer.[3]	✓ Yes, for official purposes but a. Double enveloping b. Receipt required c. Carriage by DFAT courier service or an authorised officer.[3]	✓ Yes, for official purposes but a. Double enveloping b. Receipt required c. Carriage by DFAT courier service.

[1] 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.

[2] 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.

[3] An authorised officer is an officer authorised in accordance with the policies of the SAPSF and the agencies procedures.