Table 7 Minimum protections for information transmission and transfer

<table>
<thead>
<tr>
<th>OFFICIAL: Sensitive</th>
<th>Security classified information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Low business impact</td>
<td>2 Low to medium business impact</td>
</tr>
<tr>
<td>3 High business impact</td>
<td>4 Extreme business impact</td>
</tr>
<tr>
<td>5 Catastrophic business impact</td>
<td></td>
</tr>
</tbody>
</table>

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.

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.
- Secure information from unauthorised access.

Protect information when transferred over public network infrastructure or through unsecured spaces

- Transfer over public network infrastructure or through unsecured spaces is permitted.
- Transfer over public network infrastructure or through unsecured spaces is permitted.
- Protect information in accordance with the person's duties.

Protect information from unauthorised viewing when transferred within a single physical location, eg within an office

- Transfer within a single physical location is permitted.
- Transfer within a single physical location is permitted.
- 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.
- Transfer between physical establishments within Australia is permitted.
- Protect information in accordance with the person's duties.

Protect information when transferred between physical establishments outside Australia

- Transfer between physical establishments outside Australia is permitted.
- Transfer between physical establishments outside Australia is permitted.
- Protect information in accordance with the person's duties.

Table 1 notes:

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. 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.

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 PSPF and the entity's procedures.

Guide to Securing Personal Information

Error! Reference source not found.