**Checklist for mobile and remote working**

New Zealand government employees are increasingly working away from the office.

In each instance of off-site work, agencies should consider the need to protect official resources prior to any removal of information or assets from the agency’s premises.

The following checklist can assist in assessing the risks associated with any removal and/or use of official resources off-site.

Agencies should address any security concerns raised prior to allowing work away from the office or removal of official resources.

|  |  |
| --- | --- |
| 🞏 | Has the employee been required to read, or been briefed on, the requirements for the protection of official resources? |
| 🞏 | Has the employee acknowledged in writing their understanding of the requirements for the protection of official resources? |
| 🞏 | What is the protective marking or sensitivity of the official resources to be removed? |
| 🞏 | Why are the official resources being removed off-site? |
| 🞏 | How long will the official resources be off-site? |
| 🞏 | Have the details of the official resources being removed been recorded? |
| 🞏 | Do the official resources being removed belong to another agency? If so, has that agency given its approval? |
| 🞏 | How will the official resources be securely transferred or transported? |
| 🞏 | Is the removal of the official resources from the agency a temporary/one-off or a permanent/long term arrangement? |
| 🞏 | How will the official resources be securely stored off-site? |
| 🞏 | What is known about the location where the resources are being taken? Is a risk assessment needed in relation to that location? |
| 🞏 | What control does the agency have over the security of the location? |
| 🞏 | Who has access to the location where the official resources are being stored? |
| 🞏 | How will the employee protect his/her work from unwanted scrutiny or unauthorised access? |
| 🞏 | How will the employee protect his/her official conversations from being overheard? |
| 🞏 | Could the resources being carried reasonably expose the employee to targeting by a foreign intelligence service? Has the employee been appropriately briefed? See the [Maintaining your national security clearance](https://www.protectivesecurity.govt.nz/personnel-security/national-security-clearances/maintaining-your-national-security-clearance) |
| 🞏 | Is the employee aware of what action he or she is to take in the event official resources are misplaced, lost or stolen? |
| 🞏 | Is the employee considering printing, duplication or disposal of official information in a non-secure environment? What measures have been put in place to ensure official information is not compromised by this activity? |
| 🞏 | Has the agency authorised the use of any off-site ICT equipment? If so what equipment and in what circumstances? |
| 🞏 | Does the employee have an authorised email account or remote ICT access to agency systems, that can be accessed securely? |
| 🞏 | Has the employee been required to read, or been briefed on, the requirements for the protection of official resources? |