Australian Privacy Principle 11: Security of personal information

APP 11 requires APP entities to take reasonable steps to protect personal information that they hold from misuse, interference, loss and unauthorised access, modification or disclosure.

In April 2013, the Office of the Australian Information Commissioner issued the Guide to information security: 'reasonable steps' to protect information. These guidelines provide information on the reasonable steps APP entities are required to take to protect the personal information they hold. The guidelines will also provide the basis for assessing Defence's compliance with its information security obligations under the *Privacy Act 1988* .

The guidelines address a range of areas including:

a. governance;
b. ICT security; and
c. whitelisting and blacklisting.

DSM

Within Defence all personal information must also be stored in accordance with the information security policy laid out in the Defence Security Manual (DSM), Part 2 Chapter 30 - Classification and Protection of Official Information.

Protective mechanisms include:

- Physical
  - where we store documents e.g. safes, compactus etc.
- Electronic
  - privileges - access to folders, g drives, Objective etc.

Physical and electronic security is only as useful as it is current and requires regular review e.g. when people change roles, start work with/leave Defence etc.

The DSM, along with POLMAN 3 and DI(G) ADMIN 27-4 -*Defence Records Management Policy* assist Defence to satisfy its obligations under APP 11.

To promote the security of personal information, commanders and managers should consider:

- establishing appropriate access privileges when creating new folders in Objective/G drives;
- conducting regular audits of Objective/G drive privileges;
- establishing procedures to remove people's access privileges when they leave the workplace/unit.

In addition, Defence and the Australian Government use Dissemination Limiting Markers (DLM) to identify documents containing personal information. In accordance with the DSM , documents containing personal information should be given a DLM of **Sensitive: Personnel**. Where '**Sensitive: Personal**' is used to identify sensitive health information, a warning notation of '**Health Information**' must be included below the DLM in the document to alert recipients of the requirement to handle and store the information in accordance with DI(G) PERS 16-20 -*Privacy of Health Information in Defence.*

The DSM contains an example of the **Sensitive: Personal** health information warning notation.

Taking reasonable steps to protect personal information

APP 11 requires staff to take reasonable steps to establish the basis of a request for personal information before using or disclosing the information. This may require asking the person/area making the request to explain the basis of the request having regard to APP 6.

Example: Staff responding to a request for personal information from an enforcement agency must establish why the enforcement agency is requesting the information. This could include questioning an enforcement officer on whether the information is subject to a warrant or other legislative requirement.