VPDSF INFORMATION SECURITY MANAGEMENT COLLECTION

EXTRACT OF CHAPTER 1 – APPENDIX D

SUGGESTED INFORMATION MANAGEMENT ROLES AND RESPONSIBILITIES

The following list sets out some of the more commonly recognised IM roles and associated responsibilities. Not all organisations will have these particular roles, or even describe these functions in the same way, with some smaller organisations perhaps having a single person performing a few functions. It is expected that organisations define their respective roles and responsibilities based on relevant legislative and / or regulatory obligations.

Information owner

An information owner is the person or entity that has legal possession of the information asset, and are ultimately accountable for that information. For some organisations this may be the agency or body for which the information asset was produced or acquired, and in turn the public sector body head who retains ownership of the organisations overall information assets. For other organisations, ownership may be defined in particular legislative instruments.

In some organisations, it may be appropriate for the information owner to delegate the management and handling of responsibilities associated with the information asset to an information steward and / or an information custodian.

Information steward

In some organisations this may be where an information owner has delegated responsibility for the information asset to an information steward. This person or role is responsible for making sure the asset is meeting its requirements, and that risks and opportunities associated with the information are monitored and managed. The steward, in this instance, has operational accountability for the information.

The information steward need not be the creator (originator) of the information, or even the primary user of the asset, but they must have a good understanding of what the business needs from the information asset, and how the information can help fulfill those requirements.

The information steward is often a subject matter expert, or 'owner' of the relevant business process, for a particular information collection or asset.

The role (or delegate role) should be involved in any risk assessments and analysis of the information to help assess its value[1]. Only once this assessment has been made, can the relevant security measures be considered to protect the information asset.

Information custodian

An information custodian is generally described as either a designated person, position, officer, business unit or agency with assigned responsibilities for the information asset to ensure that the information is managed appropriately over its lifecycle, in accordance with rules set by the information owner or steward and the quality of information is assured.

Information users / administrators

Any person who generates or receives official information. This can include staff or external parties who have access to the information.

1 See Chapter 2 of this Collection for steps on how to assess the value of information