VPDSF INFORMATION SECURITY MANAGEMENT COLLECTION

EXTRACT OF CHAPTER 1 – APPENDIX C

INFORMATION ASSET CONSIDERATIONS

CONSIDERATIONS	SUPPORTING COMMENTS
Business engagement	Consider how each of your business units currently use or engage with certain pieces of information in their day-to-day work. This engagement may assist you in logically grouping individual items into a broader information asset that reflects operational business needs. The use of 'like' or 'related' material doesn't have to be based on an ICT system or application, but may be informed by a business, function or activity. Some probing topics and associated questions to consider include: **Work with or use** Consider the functionality that your organisation requires from its information, how the material is used and what your organisation needs to do with it, e.g. create, modify, access, sort, store, transmit. This area may overlap with the access requirements in that there may be different groups of users who need to access the information in different ways. For example it is unlikely that your organisation will treat all the content in its large information storage system such as a records management system or data warehouse as a single information asset. These systems or holdings are likely to cover a diverse range of unrelated topics, which can mean different measures (including security measures) are needed to properly manage this information across its lifecycle. Depending on the content, certain records may be grouped into similar types. • How does the business use or work with the information? • What does the business need to do (functionality, business services, etc.) with the information? • What tools (this can be systems, hardware or software) are needed to work with the information? Usability covers everything from discoverability of the information, through how the information assets are accessed and what is done with them. Your organisation should consider current information usage requirements as well as future requirements (as these requirements may change over time). Operational record requirements (i.e. retention and disposal authorities issued by the Public Record Office Victoria) may also influence your assessment or grouping of the information asset, as well as informing retention timeframes and application of security measures across the information lifecycle.

CONSIDERATIONS	SUPPORTING COMMENTS
	Accessibility • How can the information be accessed? • What technologies, configurations and management processes are in place to access the material? • Who needs to access certain pieces of information (i.e. 'Need to know' principle, or perhaps personnel security checks are required for access to this information)? If everything within the asset is security classified, only those with the right security clearance are authorised to access or use that material. Alternatively, if only some component records are security classified then how is access to these records restricted without restricting access to the rest of the record? These requirements cover not only the security issues around people gaining access to information, but also the opportunities for sharing information internally, interoperability and sharing more widely. Discoverability • How will an organisation enable people to find the information in the way they need it? The granularity and depth of the search required will depend on the type of asset; it may involve finding the asset itself, searching within the asset for files, or searching within those files to find specific pieces of data. This is both about the technology actually used to search for information and also the technology that is used to store the information.
Business context	Consider the business context and environment in which the organisation operates. This may drive the way in which the information assets are defined and the subsequent implementation of security measures to protect this material. The nature, size and functions of an organisation will also influence the types of information assets it has.
Legal or regulatory obligations	Consider any legal or regulatory obligations that the organisation has, as these existing requirements may inform how the organisation records information elements or structures particular information sets. An example of this may include existing obligations under the DTF DataVic Access Policy[1]. Under this policy, your organisation may already be capturing metadata elements that can help you categorise and define additional information assets.

1 Organisations publishing datasets on the DataVic portal should consider the 'Dataset Publishing manual' on the DTF website.

CONSIDERATIONS	SUPPORTING COMMENTS
Business classification (records management)	Check if any of the records have a registered business classification, as this can act as a useful basis to understand various information elements (i.e. information linkages, grouping, naming, vital records, user permissions, retrieval, disposition and identification of vital records). If a record has been registered under a business classification, consider the assessment process and any information that accompanies this record. Business classification schemes assist with identifying the scope, types, use and functions of an organisation's information assets and can direct accessibility and re-usability of the material. Common business classification categories can include: • Committees • Employee relations • Government relations • Information management • Legal services • Operations management • Policies and procedures • Procurement • Risk management • Property management • Strategic management • Technology and telecommunications • Work Health and Safety. N.B. Business classifications are different to security classifications[2]
Externally sourced information	Organisations should take into account any externally sourced or generated information, as it may also be considered an information asset of the business depending on: • the functions, processes or activities that this material is supporting and • what other information this material is combined with • terms of the agreement or arrangement under which the material is supplied (i.e. does your organisation maintain ownership and IP over the information or is your organisation permitted to use this material under a copyright agreement).

2 Security classifications are a form of protective marking as outlined in Chapter 3 of this Collection. Security classifications are used to identify information that has heightened confidentiality requirements. Business classifications on the other hand are designed to support the records management needs of an organisation and act as a means of arranging records in a logical structure and sequence, facilitating their subsequent use and reference (PROS 11/09: Control Standard – 2.2 Classification).