Information Management Advice 7 Information Rights Management

Introduction

Information Rights Management is an information protection technology that allows users to place restrictions on who can view, print, forward or copy documents or email messages and the time frame in which that information remains accessible. Information Rights Management is also known as Digital Rights Management (DRM), Document Rights Management, Rights Services Management or Enterprise Rights Management.

Implications for government recordkeeping

This technology is designed to enable copyright owners to protect their intellectual property when their work is held in the recordkeeping systems of other entities. Government has an obligation to prevent unauthorised or improper use of such information. Nevertheless, legitimate copyright interests have to be balanced against the statutory requirements for government agency recordkeeping, which in Tasmanian derives primarily from the *Archives Act 1983*. Under this legislation Agencies are required to manage and preserve the evidence of their decisions and activities and it also regulates access to, and disposal of, State records. These records may include documents where the copyright is not held by the Crown.

The specific risks to good recordkeeping that are posed by DRM technologies include the following:

- **Auto-deletion** – inhibits the ability of an agency to capture and maintain full records of its business. For example, the sender of an email can stipulate the lifespan of a message and force the deletion of the message from the system at a predetermined time. Automatic deletion (not involving human intervention) of messages received by government agencies is most likely to result in unauthorised disposal.
- **Print disabling** – for agencies maintaining records in paper format, this prevents them from creating and maintaining proper records.
- **Forward disabling of email messages** – prevents capture into many systems thereby preventing agencies capturing records of business.
- **Encryption** – through loss of keys and passwords, encryption can prevent access and therefore results in the effective loss of records to government and the public.
- **Security** – each time a protected object is accessed, there is communication between

DRM systems and external rights services, which may affect information security and access provisions.

Advice for government recordkeeping

The State Archivist does not endorse the use of information rights management to enable the automatic deletion of documents or email messages, or to place restrictions on documents/messages that may impede recordkeeping practices. State and local government organisations are advised they must not use this functionality.

If your organisation is receiving information rights protected documents and messages from other organisations, it is recommended that the documents/messages have all rights protection controls removed from them prior to their capture into recordkeeping or document management systems. This may involve requiring the sender to re-send the document/message or to use an alternative format or communication method.

Further Advice

For more detailed advice please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History
Build Status

Version	Date	Author	Reason	Sections
2.0	February 2015	Christine Woods	Template	All
1.0	15/07/2009	AOT	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
All	All	Document imported in to new template

Issued: July 2009

State Archivist