

Public Records Brief

A RECORDKEEPING UPDATE FOR QUEENSLAND PUBLIC AUTHORITIES – FIRST ISSUED SEPTEMBER 2004
REISSUED IN NEW FORMAT FEBRUARY 2008

What is Microsoft Information Rights Management?

Information Rights Management (IRM) is a component of the Microsoft Office 2003 product suite. IRM allows document authors to specify who can read their document, what they are able to do with the document, and when they are able to do it. IRM can be applied to Outlook emails, Word documents, Excel spreadsheets, and PowerPoint presentations. IRM is not available for Microsoft Access databases.

Without IRM, documents circulated electronically are uncontrolled and can be printed, copied, and forwarded feasibly to anyone. Transmission of emails and documents over secure networks may protect the information in transit, but offer no control over what the recipients do with the information. Password security protection for documents can easily be circumvented if the password is also provided.

IRM can be used to prevent the printing or forwarding of emails and to make them inaccessible to the recipient after a specified expiry date. IRM can make documents unreadable by anyone other than the specified recipients.

How is Information Rights Management deployed and used?

Deployment of IRM is performed across an organisation at the server administrator level. In addition to the Microsoft Office 2003 client software, Microsoft Windows Server 2003 Enterprise Edition, Microsoft Windows Rights Management Server for Windows Server 2003, Microsoft Active Directory Services, Microsoft Internet Information Services, and Microsoft SQL Server 2000 all need to be acquired, installed and configured for IRM¹.

The server and client PCs need to be loaded with the Rights Management Update for Windows. Public and private keys for creators and readers are created when the users enroll to use the Rights Management Service (RMS). Microsoft Office Professional Edition 2003 is required to create rights protected documents, but they can be viewed with other editions of Microsoft Office 2003, or with the IRM add-on for Microsoft Internet Explorer. IRM does not work on Terminal Server thin client environments or on non-Windows operating systems such as UNIX or Apple².

By default, when Microsoft Office 2003 is installed, IRM is not enabled. Without the additional software listed above, end users will not be able to create rights-protected material. Even if this infrastructure is in place, the application of IRM should be controlled at a central level through computer access policies and permissions.

RMS policies are established and promulgated by systems administrators. It is up to the end user to apply the appropriate policy to the document they are sending, by pressing a button and specifying recipient rights. Emails can still be sent and documents can still be created and distributed without any rights management applied to them.

¹ *Enabling Information Protection in Microsoft Office 2003 with Rights Management Services and Information Rights Management*. (2003). © Microsoft Corporation. Accessed April 2004 at <http://www.microsoft.com/technet/prodtechnol/office/office2003/maintain/rmsirm.msp>

² Turick J. (2003). *Information Rights Management in Microsoft Office Outlook 2003* © Microsoft Corporation. Accessed April 2004 at <http://support.microsoft.com/default.aspx?scid=kb:en-us:831498>



At this stage, no government agencies in Queensland have commenced widespread deployment of this technology. IRM seems to be most useful within large organisations to prevent the flow of sensitive information to unauthorised staff or people outside of the organisation. Many of the features require access to server components that would not usually be accessible outside of an organisation's internal network. Therefore, if IRM protected information has been sent externally, even intended recipients may not be able to read the content.

Why is Information Rights Management a concern?

Lack of a thorough understanding and rumours about IRM have caused record and document managers concern over this new software component. Microsoft admit that there is confusion and a lack of clarity regarding IRM functionality, particularly the widely held belief that messages will 'self-destruct' or vanish into thin air³. The setting of an expiration date for an email or document means that after a specified date, only administrators or document authors will be able to access the documents. The message or document is not destroyed; it actually remains on the server in its original state⁴.

Despite this explanation, there is concern in the archival and records management community that IRM may interfere with records management software and/or procedures used to capture, store or search official correspondence. Others are concerned that implementing IRM forces people to adopt Microsoft solutions⁵, since in addition to the various software components required to implement IRM, it is suggested that recipients have a Microsoft Hotmail® email address and Microsoft Passport to allow verification of credentials for remote access to IRM enabled documents⁶.

What is the recommended action for agencies?

The Queensland State Archives (QSA) will work with Government ICT in the Department of Public Works, Microsoft Australia and other key stakeholders to gain a thorough understanding of the technology and its implications.

With the volume of information used in an electronic form increasing rapidly, the compatibility of other systems (such as electronic document and records management systems) to access information that has been protected with IRM is critical. It is also important for Queensland public authorities to ensure that the application of IRM does not hinder any accountability requirements to capture, create and store public records in electronic formats.

Agencies are advised to conduct their own business and technical evaluation of the technology to explore the issues detailed in this document prior to their implementation of IRM. It is also recommended that agencies consult with QSA to ascertain current research and policy directions regarding the technology. A further guideline on the use of Microsoft Information Rights Management may be provided.

³ Finlayson S. (2004). *This Message will Self Destruct*. Image & Data Manager Magazine. January / February 2004. © Knapp Communications Inc.

⁴ Finlayson S. (2003). *Microsoft Refute Self-Destruct Email Claims*. Image & Data Manager Online. © Knapp Communications Inc. Accessed April 2004 at <http://www.idm.net.au/storypages/story-records.asp?id=4824>

⁵ Dunovant E. (2003). *Microsoft Information Rights Management - Threat or Menace?* Accessed April 2004

⁶ Turick J. (2003). *Information Rights Management in Microsoft Office Outlook 2003* © Microsoft Corporation. Accessed April 2004 at <http://support.microsoft.com/default.aspx?scid=kb:en-us:831498>