



SECLORE

Why Content Repositories need IRM

A WHITE PAPER



SECLORE



Why Do F1 Cars Have The Biggest Brakes?

Because They Need To Go The Fastest.

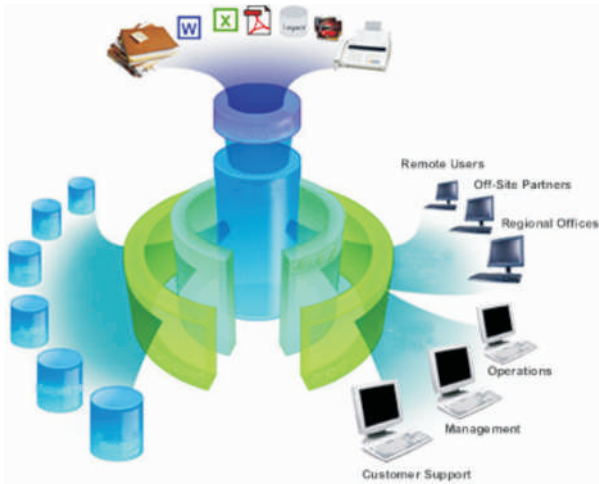


INDEX

<u>Introduction</u>	1
<u>Security of Info within Content Repositories</u>	2
<u>Information Rights Management</u>	3
<u>Securing Information with IRM</u>	4
<u>Benefits of IRM Integration</u>	6
<u>Contact us</u>	7

Why Content Repositories need IRM

Introduction



Today, organizations worldwide are being bombarded by volumes of information flowing through email, internet and mobile devices. There is a continuous inflow and outflow of documents being created, transferred, modified, stored and disposed. Enterprises invest in sophisticated collaboration tools to reduce and manage document flow. The systems come in different flavors like electronic content management (ECM), business process management (BPM), knowledge management (KM) and document management

systems (DMS) which, for our purpose, we will refer to as Content Repository.

In most cases, Content Repositories have been deployed within the enterprise for intra-enterprise collaboration. The need and deployments of content repositories is now quickly expanding to go beyond the enterprise and involve business partners, vendors and sometimes even customers. This however, has left the information contained within the repository vulnerable to mass leakage. The volatile nature of business relationships also means that information and systems shared with business partners are used in accordance with pre-defined norms. Ensuring the security of information through the lifecycle of creation, distribution, use, and destruction thus gains importance.

Information rights management (IRM) systems like the ones by Seclore (Seclore FileSecure), Microsoft (Microsoft RMS) and Oracle (Oracle IRM) when deployed along with Content Repositories empower enterprises with the ability to robustly secure and monitor access to content and information within and outside of the repositories.

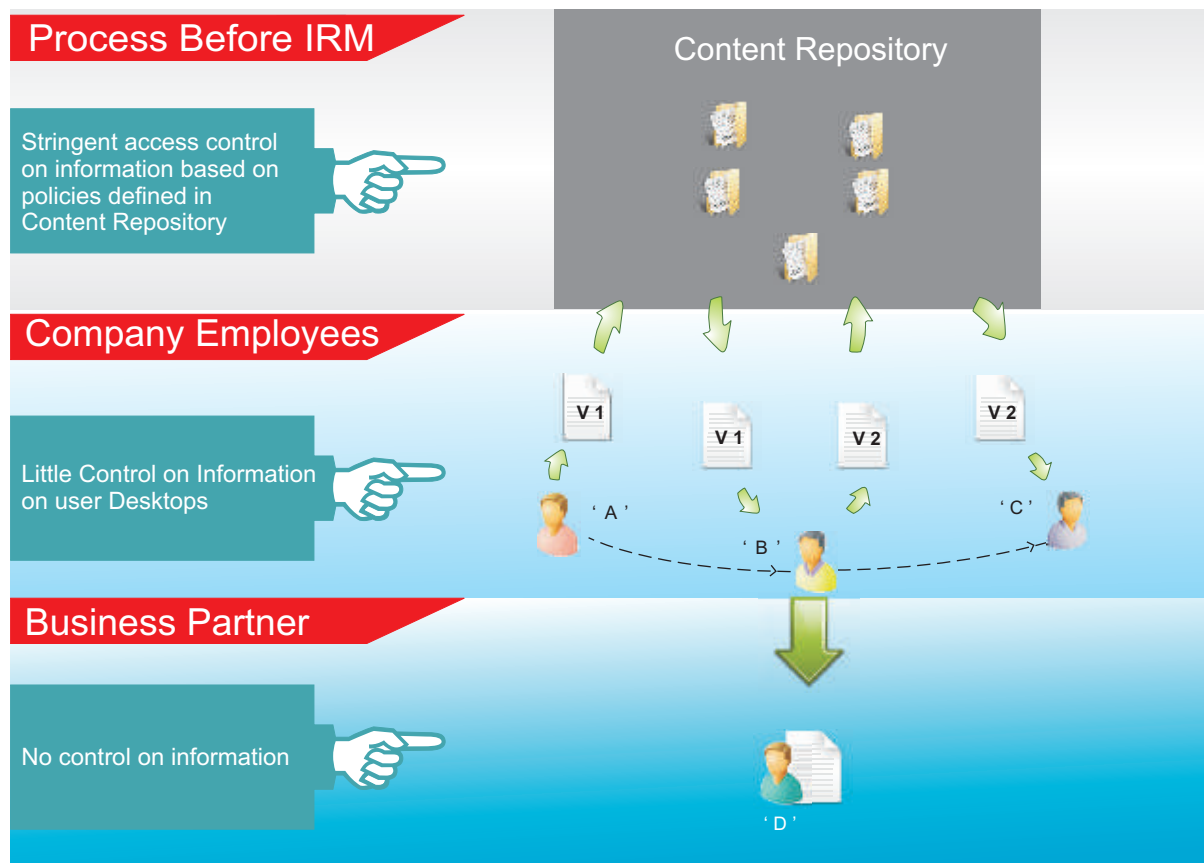
Why Content Repositories need IRM

Security of Information within Content Repositories

Security policies for information contained within a content repository are only applicable till the time the information is resident within the repository. Repositories therefore implement only the first level of security called “access control”. Access control policies dictate whether a user can download information from the repository or not. Once the access control is given and information is downloaded, repositories don't have control over what the user can do with the document (e.g. can he print, edit, copy content, and/or distribute the information). Access control therefore does not protect the information but just the “gate” through which the information can leave.

By losing all control of information when it moves out, the repository also cannot track distribution and usage of the information thereafter. Last, but not the least, changes done on the access control policies get implemented only for subsequent download/use of content. These changes cannot be forced by repositories for content that is already downloaded.

Because of all the above factors and by virtue of its perimeter-centric nature, information in content repositories frequently gets breached intentionally or unintentionally. Depending on the nature of the business this could pose an threat to the business and the ROI achieved from the content repository.



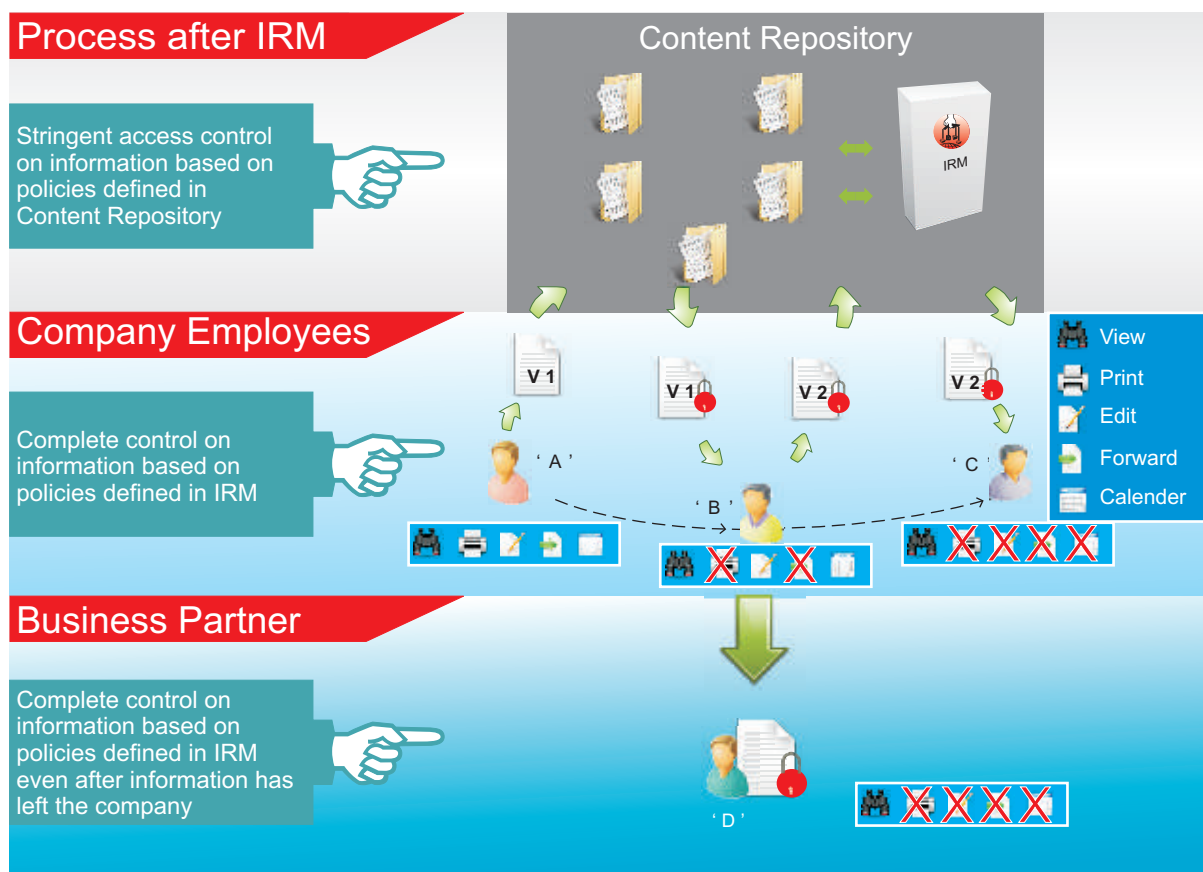
Why Content Repositories need IRM

Information Rights Management

IRM technology enables “owners” of information to control the actions that are performed on the information once it has been downloaded from a content repository. IRM protects the information and restricts usage to only specific users or groups, specific actions like view, print, edit, copy content and distribute, specific time of usage like “till 19th August 2009” or “2 days”. In some cases IRM can also restrict the usage to specific computers and network IP addresses thus providing an additional layer of control when providing access to systems outside of the enterprise.

These controls are applied to the content itself without any constraint on the computer, network, storage or transmission technology used. In most cases the controls are also dynamic, for example if the “owner” wants to change the controls to provide usage to a different set of people, different set of actions, etc., it is possible for him/her to remotely change the rights to all copies of the information.

One of the core benefits of IRM technology is that it implements security and control irrespective of the location of the content within or outside of the enterprise. Unfortunately, some IRM technologies make inter-enterprise collaboration difficult by making external user access difficult.



Why Content Repositories need IRM

Securing Information with IRM

Securing information with IRM involves manually or automatically defining “usage rights” for the information as it leaves the repository.

Usage rights are a combination of the following controls:

WHO can access the information: This typically relates to a user repository like an LDAP system and also maps the organization hierarchy of users, groups & organization units. For some IRM technologies, it is also possible to link this to non LDAP user databases as defined in custom applications and portals.

WHAT can each user do with the information: This typically relates to individual actions allowed on the information by the specific user. Individual actions which can be controlled are viewing, editing, printing, forwarding/sharing, copy/paste of content and un-protecting.

WHEN can each user access the information: This control can limit users to access the information within a specific date range or time span. A document could thus have “19th August 4 pm to 23rd August midnight” as a specific date range or “2 days from first access” as the specific time span within which the document is available.

WHERE can the information be used: Even within IRM technologies, this is not-so-commonly available feature which could become useful in cases of information of extreme confidentiality. This control can restrict usage of the information to only a pre-specified list of computers identified by the hardware or to a specific range of IP addresses or networks.

Hence consider the case of a simple Workflow consisting of a document preparer (A) → document reviewer (B) → and document approver (C).

The usage rights matrix for a downloaded document of such a workflow would typically look like:

WHO		WHAT			WHEN		WHERE
User	View rights	Edit rights	Print rights	Distribute rights	Date Embargo	Location	
A	✓	✓	✓	✓	X	Anywhere	
B	✓	✓	X	X	X	Anywhere	
C	✓	X	X	X	✓(only after a certain date)	Within the office	
D	✓	X	X	X	✓(only after a certain date)	Within the office	

Why Content Repositories need IRM

Content Repositories	Content Repositories Integrated with IRM
<i>Can control access to information only when it resides within</i>	<i>Can remotely control WHO, WHAT, WHEN, WHERE of information</i>
<i>Cannot change access rights on information post download</i>	<i>Can change the controls on information post-distribution</i>
<i>Cannot track usage of information post download.</i>	<i>Can track all authorized and unauthorized attempts on information</i>
	<i>Is independent of mode of transfer & location of information.</i>

In most cases the above usage rights are seamless and transparent to the end user. The user's experience, as long as his actions are permitted by the system is also exactly the same as before. Documents uploaded into the repository can be automatically protected based on the user and the location in which they are placed. The single sign-on mechanism allow users to access the documents without the overhead of yet another user ID and password.



Why Content Repositories need IRM

Benefits of IRM Integration



Integrating IRM into repositories brings tremendous security and benefits to the enterprise. IRM provides complete and persistent usage control on information throughout its life cycle. Security can now be ensured without compromising on the collaboration capabilities of content repositories.

One of the major benefits of IRM is its audit trailing mechanism. IRM can audit trail the usage of the information once it leaves the repository. Authorized actions as well as unauthorized attempts could be tracked across enterprise boundaries. This can help

enterprises to adhere to regulatory and compliance frameworks like ISO, Sarbanes-Oxley and HIPPA for “unstructured” data control.

IRM can also significantly lower costs and process delays associated with version control and document retention policies. With IRM, information can be shared with employees and business partners with no large additional investment in security systems. It increases revenues by preventing misuses, theft and leakage of “paid” content.

The integration of IRM with content repositories makes information-centric security for all confidential content an achievable aim. The minimal cost and effort of having such a necessary and must-have feature outweighs the risks of losing sensitive information.

Security and collaboration are usually considered mutually conflicting goals. IRM proves this to be a myth.

Why Content Repositories need IRM

About Seclore

Seclore Technology is a high growth security software product company, providing security solutions in the areas of information usage control, Information Rights Management (IRM) and secure outsourcing.

Seclore's expertise lies in the control of information post distribution, irrespective of location and mode of transfer. The receiver is able/not able to distribute, edit, print, copy-paste, screen-grab information from the document. It is also possible to remotely destruct the documents at the receivers end.

Some of the largest companies in banking and financial services, insurance, engineering services, educational institutes, among others, use Seclore's technology to secure data that is used internally or provided to a vendor for outsourced processes.



SECLORE

Call: +91-22-4015 5252

info@seclore.com