

# Mobile Content and Document Management Best Practices and Decision Checklist

Enterprise-Grade Solutions Give IT Much-Needed  
Security and Control Over Company Content



# Table of Contents

---

- 4 **Everyone's Going Mobile**
  - Users and IT Agree on Mobile Content Management
  - Mobile Content Management Use Cases
  - How IT Can Respond to Mobile Content Management Concerns
- 6 **Mobile Content Management Best Practices**
- 7 **Mobile Content Management Decision Checklist**
  - MCM Feature Requirements

A typical executive will store her business group's budget, product road map, customer database, and dozens of presentations, Word docs, and spreadsheets on her mobile phone, tablet, or laptop. Accessing, sharing, and updating her mobile work content is status quo. That's how she and her peers stay productive. What she probably doesn't realize is that the business content she's taking into airports, client sites, doctor offices, restaurants, and home is a ticking time bomb.



# Everyone's Going Mobile

---

Every minute of every day, employees move business files onto their mobile devices so they can work at home, on the road, or at client sites. Salespeople, engineers, executives, bankers – they simply reach for their smartphones and tablets to share, review, approve, write, read, edit, present, and perform countless other work-oriented activities. They store presentations, Adobe PDFs, videos, Word docs, spreadsheets, and music on all types of mobile devices from iPhone and iPad, Android, BlackBerry, laptops, notebooks, and tablets. The result is the equivalent of a mobile scrum of risks, redundancies, and wasted efforts and resources.

This mobile content quandary is a result of the huge popularity of mobile phones and tablets and the bring your own device (BYOD) trend. According to current research, more than one billion workers will be using mobile technology by 2015. Today, each person is carrying an average of 3.5 devices, and workers are gravitating toward tablets.

With so many mobile devices and so much content, businesses are at risk. Mobile device management provides a first defense, but it's not enough. Businesses need to lock down the content and documents with policy-based controls to decrease their level of risk and ensure comprehensive enterprise mobility management. The combination of securing devices and content greatly reduces risks. IT can secure the business content that is stored on mobile devices through mobile content management, or MCM.

## USERS AND IT AGREE ON MOBILE CONTENT MANAGEMENT

The mayhem caused by insecure mobile content ripples across both users and IT, as well as through the business. From the users' point of view, they need an easy-to-use process for accessing and seamlessly syncing content from their mobile devices. Many are using a consumer-based tool such as Dropbox to transfer documents, or they are manually moving files via iTunes or e-mail. They rely on these tools because they need to access their working documents from their mobile devices, and they want to share the content across devices and across users. These files become especially tangled when a team is attempting to collaborate.

Many companies prohibit the use of these tools. But employees create workarounds, often e-mailing files to personal accounts – a tedious process – or ignoring company policies. They need a better way to access their mobile content.

## MOBILE CONTENT MANAGEMENT USE CASES

Employees across all industries and lines of business require access to corporate content. For example, in the aviation industry, pilots are required to carry navigational charts, log books, and other reference materials with them on every flight. Several major U.S. airlines have already moved to tablets, and other airlines are expected to follow. A mobile content management system can help

make sure the documents on the tablets are the most current versions. When a new guideline is approved, content owners will update the manuals and push it to the pilots immediately. In other industries, pharmacists, service professionals, life insurance agents, stockbrokers, and many others who depend on having updated, relevant information at their fingertips will find mobile content management systems extremely useful.

Mobile content management makes collaborating on a document much easier than sharing over Google docs or e-mail. A marketing lead, for example, can share the first draft of a product brochure with all stakeholders. Before sending it to the group, the lead assigns rights to each recipient. Because the product is not publicly released, the marketing lead adds a security layer by setting the document as highly classified, which prevents it from being forwarded or stored offline.

## HOW IT CAN RESPOND TO MOBILE CONTENT MANAGEMENT CONCERNS

IT needs to respond to mobile content management concerns. Many businesses have lost control over their corporate data, and in many cases are extremely vulnerable. This breakdown hit organizations hard in 2011 when a security failure at a file-sharing company exposed the files of millions of customers. Hackers continue to steal user names and passwords and use them to access data. IT can respond to these risks by adding enterprise-grade security that supports authentication controls, encryption, usage reports, and rights-controlled sharing. If IT doesn't provide a way to access and share the content, users will continue to go rogue. Employees know how to sync files and share them across devices and groups. IT needs to step in and provide them the same easy-to-use tools with enterprise-grade security and management features that the current set of consumer-based tools are sorely lacking, including:

**Encryption:** Documents need to be encrypted when they are being transferred and when centrally stored.

**Authentication:** To keep the enterprise safe, users must be authenticated through identity management. This is especially important in large-scale deployments, and can use the information, groups, and roles that enterprises have already established.

**Rights-controlled sharing:** By classifying each document as confidential, internal, customer, public, and so on, and assigning specific security policies, such as open, present, e-mail, view only, contribute, and more, IT keeps a tight hold on who is accessing business content. Rights can also be based on device used, content, and geographical information.

**Reports and auditing:** Usage stats of who is accessing what content and when help enterprises track content and remain in compliance. In many industries, compliance regulations require knowledge of how, where, and when content is used and managed. MCM auditing tools provide this must-have information.

**Data loss prevention:** Because mobile devices are lost and stolen every day, and employees move on to jobs at other companies, IT needs remote-wipe capability to remove business content from the devices. MCM systems allow administrators to delete users' accounts to prevent unauthorized access to business content.

**Group-based collaboration:** With this capability, content owners can push updated content to teams to make sure they have the latest versions. Content owners can also provide team members different access rights to finalize project documents.

**Separation of personal and business documents:** Enterprise solutions separate personal from business by moving them into containers.

The need for mobile content management starts with security, but it expands through the enterprise to encompass management of mobile devices and content, control of documents and user access, and collaboration and productivity. When mobile content management is combined with mobile device management (MDM), businesses are well on their way toward full enterprise mobility management. The mobility tide is getting bigger and stronger, and enterprises with the most advanced mobile tools and resources will be ready to take advantage the greater productivity, increased efficiencies, and improved operations that come with a mobile enterprise.

# Mobile Content Management Best Practices

---

Mobile content management is a significant step in enterprise mobility management. When planning to implement an MCM strategy, follow these best practices.

- 1. Assess your current situation.** Interview a broad cross section of your employee base to fully understand your enterprise requirements. Find out what mobile devices they are using, what tools for sharing and accessing content, and the types of content. You can get this information through group discussions, surveys, interviews, and from Internet proxy logs. Your security risks – and user needs – should become quickly apparent.
- 2. Be afraid of the unknown.** What you don't know can hurt you, and consumer-oriented content-management tools keep you in the dark about what's happening to business content. Consumer-based apps lack enterprise dashboards that provide much-needed insight into mobile content activity, including a usage audit and activity tracking. They are also missing identity-based access, security controls, encryption of content, and the ability to separate business documents from personal documents. An enterprise MCM system takes the fear out of the unknown.
- 3. Don't rip and replace; maintain your existing content management investments.** Extend the content you have from where it sits today. Leverage your investment in enterprise content management solutions, such as Microsoft SharePoint, OpenText Document Management, EMC Documentum, and others.

- 4. Establish file-sharing policies that make sense for your industry.** Consider your industry, employees, and business goals as you define your file-sharing policies. Regulated industries such as finance, healthcare, pharmaceutical, and aviation will have much stricter policies than the consumer products and retail industries, for example. The first action is to assign employees to groups based on their roles and the types of content they need to access. Next, you will need to categorize content and segment it as "highly classified," "classified," "open," and so on. Each classification will have unique security controls; for example, highly classified documents cannot be forwarded, stored offline, or shared. These types of policies help ensure that you meet industry regulations and prevent your business content from becoming a security risk.

- 5. Consider the impact of BYOD in the enterprise.** As employees bring their personal mobile devices into the workplace, security risks skyrocket. You can lower the risks by securing the business content that employees want to store on these personal devices and separating personal and business content. If you don't give users a corporate-approved, safe mechanism to access both their personal and business docs, they will use the consumer-based tools and put the business at risk. You can further prevent critical business data from being deleted or accessible from a lost or stolen device by coupling MCM with MDM.

- 6. Audit content usage and corporate-distributed content regularly.** Enterprise dashboards provide a rich set of usage stats that clearly identify who is accessing what and when. Industries with strict compliance regulations should review usage frequently, often on a daily or weekly basis. A regular monthly audit, reported to each line of business, will provide enough information for less-regulated industries.
- 7. Train users in the importance of securing content and how to share content safely.** The majority of your employees probably already use Dropbox or another consumer solution. These tools are easy to use and help employees be productive. What people don't understand is that they put the company at risk. Rather than force another corporate rule onto users, educate them on the risks of using the consumer tools and provide good training on the corporate MCM system. Giving them the why and how will make them believe in and adopt MCM best practices.

# Mobile Content Management Decision Checklist

---

Mobile content management is essential for enterprises that are:

- Establishing an enterprise mobility management strategy
- Experiencing the BYOD phenomenon
- Looking for ways to secure and control access to business documents and content from mobile devices
- Needing reporting, auditing, and authentication controls for mobile content
- Recognizing that they need to replace risky, consumer-based options currently in their workplace

## MCM FEATURE REQUIREMENTS

When researching and evaluating an MCM system, look for the following must-have features. The MCM market is maturing, so investigate product road maps and watch for new features to be added that will further improve mobile content accessibility, security, management, and collaboration. For now, find an MCM system that:

- ✓ **Supports market-leading mobile devices and operating systems** – Syncs content across Apple iOS, Android, and Windows phones and tablets, Windows and Macintosh desktop and laptop clients, and HTML5 user interfaces.
- ✓ **Secures access to corporate content and personal files** – Separates personal content from the business files and protects all data deemed for business use. It also needs to remove user rights immediately when the device is lost or stolen.
- ✓ **Ensures control over corporate data** – Encompasses the full security lineup: encryption, authentication, compliance, and adds that additional layer by assigning role-based rights so employees only

get to access the specific documents they need and are approved to access. Identity management integration is an absolute necessity.

- ✓ **Provides exceptional user experience** – Allows employees to easily and reliably access, sync, and collaborate on multiple content types, including videos, documents, spreadsheets, presentations, customer data, and more at any time, from anywhere.
- ✓ **Enables and promotes team collaboration** – Enables employees to view, present, and collaborate on shared documents, and content owners to publish documents to specific user groups.
- ✓ **Delivers visibility and insight into mobile content usage** – Identifies who is accessing corporate information, when, and how with easy-to-read, detailed reports and usage records and dashboards of corporate-distributed content.
- ✓ **Simplifies access to enterprise content management platforms** – Works seamlessly with Microsoft SharePoint, the SAP NetWeaver® Portal component and Knowledge Management function, OpenText solutions, Documentum, and other platforms so users can continue to find and access their content easily.
- ✓ **Adapts to cloud, on-site, and hybrid data environments** – Enables access to your content and systems from wherever your employees are located. You should not need to change your environment.
- ✓ **Is built on open, interoperable systems** – Enables you to employ this system as a hub for all your mobile content. It will need to adhere to industry standards, especially content management information systems.

## LEARN MORE

SAP offers mobile content management solutions that provide secure access to corporate content. Find out more at [www.sap.com/MDM](http://www.sap.com/MDM).

**CMP24361 (13/02)**

© 2013 SAP AG or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.

