5 Tips to Maximize Mobile Productivity with Microsoft Office Documents

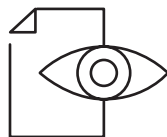## Enable Secure File Sharing and Mobile Productivity

Microsoft Office is a staple on business desktops around the globe. Knowledge workers rely on PowerPoint, Word and Excel on a daily basis. As these users increasingly adopt mobile devices to improve customer engagement, productivity and work-life flexibility, they need a solution that provides similar desktop quality for viewing, editing, saving and sharing Microsoft Office documents while on the go.

For IT, providing an easy and intuitive experience for document management is just one key requirement.

Selecting the right solution for mobile content management involves understanding the key use cases, including:

- executives viewing attachments only
- marketing professionals creating and editing content
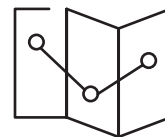- salespeople requiring offline access on planes

And, of course, ensuring that corporate data in the documents is protected at all times.

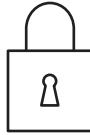Here are five critical capabilities to look for:

1. Ensure an Optimal Viewing Experience

A picture is worth a thousand words, but if the quality of that picture is grainy with key details left out, it's not that useful. Many users have had poor experiences working with documents on their mobile devices due to rendering software that does not deliver high-quality visualization or editing capabilities. If your solution doesn't deliver a near desktop viewing and editing experience, users will reject it. For mobile users, Microsoft® Office Web Apps offer the closest-to-desktop experience when the documents are viewed within a browser on the device. However, users also work offline so enabling offline editing with a high quality, consistent experience across iOS® and Android™ devices should also be considered.

2. Support all Key Document Workflows

How do most document workflows begin? The answer of course is email. Users want the ability to download, view, edit, save and send email attachments from within the mobile email client. They also need to save the attachments to SharePoint® or locally on their device for later review. Users should also be able to navigate, right from their mobile devices, directly to SharePoint® or OneDrive to access and edit documents. However, many businesses rely on other file repositories as well, such as network file shares or cloud storage, so your mobile solution should also provide access to other common repositories.
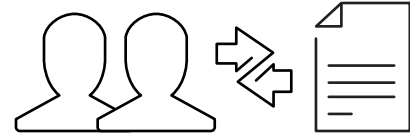
3. Protect Documents Stored on Devices

Your corporate data is your intellectual property. Many users that you have enabled with mobile email — executives, finance and sales professionals — deal daily with sensitive corporate information such as customer contracts, financial statements and sales forecasts. Preventing data leakage of these sensitive corporate documents is key to maintaining corporate reputation and customer loyalty. A secure container protects data within the app (such as an email client or browser) and as it moves through your enterprise infrastructure. But not all containers are created equal. Look for a solution that protects content, as well as the corporate credentials and configuration information on your users' devices. Corporate credentials and configuration files contain information such as Exchange, Wi-Fi and VPN credentials, which if lost, could allow unauthorized entry to your organization.

4. Make Document Sharing Easy

Mobile users often need to edit a document and then send it to a client or colleague. PDF files are optimal for mobile — they preserve the formatting, can prevent editing by the recipient if needed, and also reduce the file size, which is essential when connecting over a low bandwidth wireless network. Ensure your solution provides users the option to convert documents or attachments (including their PowerPoint presentations and Word documents) to PDF files so they can easily save them back to a file repository. Give them the option to download, edit and then send back as attachments using a secure mobile email client.

5. Protect Documents Shared Off Devices

Inevitably documents leave the device. They are sent in email or uploaded to repositories. In addition to ensuring documents are containerized on the device, ensure once they leave they are equally well protected. Document-level controls via digital rights management (DRM) can be used to restrict access to particularly sensitive files, to track where files may go, and to revoke access to a file if necessary. Look for a solution with robust DRM controls managed from the same console where you manage your containers. This will give you the maximum level of security for different user populations, use cases and file sensitivities while reducing your burden on IT.

Mobile content management for Microsoft Office documents is a key challenge and opportunity to drive mobile adoption. If the solution you choose can deliver on the requirements outlined here, you're on the right path to improving business productivity and satisfying users without compromising corporate data security.

About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world's most sensitive data across all end points — from cars to smartphones — making the mobile-first enterprise vision a reality. Founded in 1984 and based in Waterloo, Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The Company trades under the ticker symbols "BB" on the Toronto Stock Exchange and "BBRY" on the NASDAQ. For more information, visit www.blackberry.com.