M-Files
The Smarter Way to Work.

eKMS



The Ultimate Guide to Remote Work Efficiency



What's the best way to work efficiently from home? What are the technology tools needed to maintain continuity and productivity? These have abruptly become pressing questions as employers around the world tell staffers to work remotely.

It can be difficult, particularly in small spaces or when other house members are also working from home. Technology has made remote work viable, but the focus on which tools to implement can be broken down into two phases:

Short-term solutions to maintain continuity. Point solutions are being propped up quickly to ensure that business can at least continue in some form or fashion. Employees still need to have meetings, collaborate on projects and access critical information. As a result, in the interest of scaling a remote workplace rapidly, organizations turn to quick-fix solutions to solve the immediate need. These Band-Aid measures are important but may jeopardize information governance protocols, compliance and security, if not monitored for adherence to company protocols.

Long-term strategy for a flexible workplace. The next phase is to implement a flexible workplace strategy that ensures a level of business continuity commensurate with any world event or sudden need to deploy masses of knowledge workers remotely. Developing a well-formed, overarching strategy — one that promotes a cohesive working environment while adhering to governance, compliance and security protocols — creates a truly flexible workplace that outlives any one-off event. The idea is to have a sustainable infrastructure where, in the best scenario, knowledge workers have all the technology tools they need to simply grab their laptop from the office and work from anywhere they happen to be. Ultimately, with technology, companies should empower their remote staff to have the same — or similar — work experience remotely that they would have at a brick-and-mortar office space.

In this whitepaper, we present a variety of technology tools needed to deploy a remote workforce — the bare minimum requirements. More importantly, we'll carry the discussion one step further — exploring how to create a viable technology strategy to ensure continuity, productivity and efficiency.

Short-term solutions are reactive.

Long-term strategy is proactive.

M-Files

Must-have technologies & tools to enable a remote workforce

- The basics
- Communication tools
- Collaboration tools
- Security tools
- Information Management tools



The basics

Most of these requirements are obvious, but, without the following hardware, any list of essential tools would be incomplete.

Laptop

First and foremost, knowledge workers need a computer. Desktop is fine, but laptops are better for portability — a computer with decent processing speed and essential software — like Microsoft Office — is step one.

High-Speed Internet

Again, obvious, but knowledge workers should have a high-speed internet connection at their homes.

Headset

Equip your knowledge workers with a good headset for meetings and conference calls, lest they sound like they're 100 feet away from the microphone.

Webcam

Most laptops come stock with a webcam these days, but if not, instruct them to find one for use with video conferencing applications.



Communication tools

People need to come together for meetings. They need to ask their colleagues a question. They need access to their teammates. The de facto communication tool in most companies is email. But email is being cannibalized by a new breed of instant communication tools that enable teammates to chat with one another in real-time.

Companywide Chat.

When water cooler catch-ups aren't possible, teams will need a new tool for quick and efficient communication — and that tool needs to be uniform and deployed companywide.

Without a central chat hub, your teams will go rogue and may start using other channels (did anybody say WhatsApp?), further limiting their capacity to focus and potentially creating troubles with tools that are not under the control of IT.

Different departments communicating in silos — like email, texting, personal Skype accounts — leave key stakeholders unaware. Not only that, but any information they share with one another over those channels — files, documents, conversations — leaves the purview of the organization and becomes siloed, as well. Instituting one, companywide chat tool eliminates confusion and repetition and might conform better to established information governance protocols.

Make sure the communication & collaboration tools you choose aren't furthering information sprawl.

Despite the hype, though, instant communication tools are not the magic wand to fix remote work. As for most solutions, they can't just be rolled out with the hope employees will use them intentionally and productively. That's why it's important to work on a set of guidelines, mainly around the following four topics.

Develop a common format for channel and group chat names. For example, project-based channels may have a common prefix like "Project-XYZ Corp". This helps organize your communication workspace and is especially helpful if you're spinning up several new channels in a short period of time.

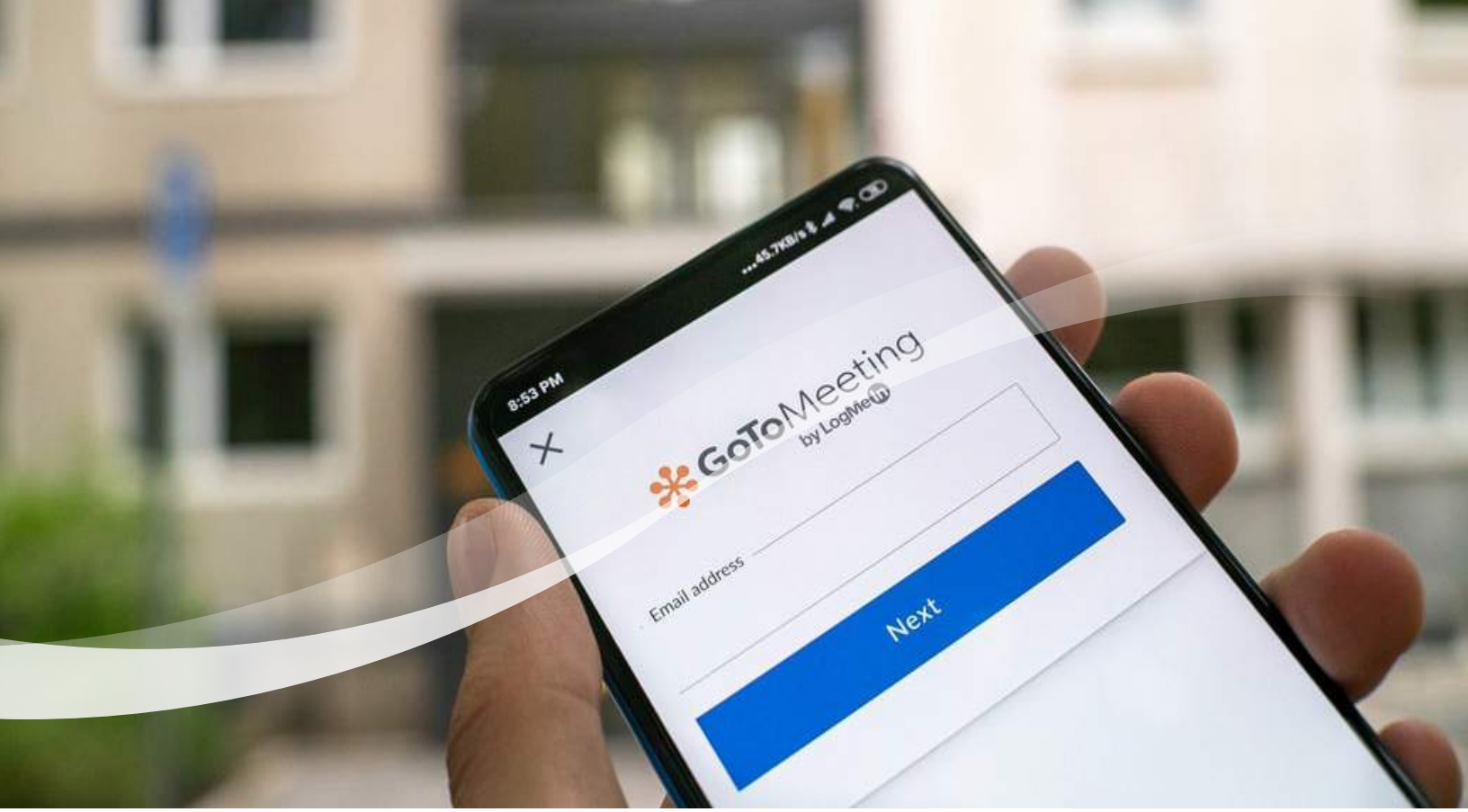
Make use of features. Any chat engine worth its salt should allow for some rich functionality — status, apps, document storage, and more. These features are often overlooked, but they can help make the chat tool feel like an integrated part of your workflow and less of a distraction.

Customize notification settings. It is incredible how this gets often ignored, considering how much we complain about instant notifications disrupting our focus. Chat tools offer a wide range of customization to make sure you only get the notifications you need, and companies should instruct their employees to do that appropriately.

Thread your responses. Channels get noisy and conversations get lost in the mix. Encourage employees to respond in-thread (UIs often do not make this easy) to keep things organized and maintain sanity.

COMMON EXAMPLES:

slack



Video Conferencing.

Meetings don't stop just because staffers are working remotely. They still need to communicate with teammates, clients, prospects, and external contributors. When in-person meetings aren't a possibility, real-time video chat is the next best substitute.

Some organizations are adopting a webcam-on policy to make remote meetings feel more engaged and personal. That is a good habit to take, particularly at the beginning and at the end of a meeting: seeing your teammates increases the sense of closeness and normalcy. During the meeting, though, you might want to turn the cameras off, to increase focus and limit bandwidth consumption.

As with chat tools, the tool for video conferencing should be uniform. In fact, the ability to meet via video conference is stock functionality with the major chat tools.

COMMON EXAMPLES:

slack Teams zoom GoToMeeting

Collaboration tools

Group work is done in the context of projects — broken down into individual tasks that each have their own contributors and characteristics. When knowledge workers are deployed remotely, they should be equipped with a toolset that allows them to keep track of all the moving parts of a project:

Timelines

Resource allocation

Budget considerations

Individual tasks and group tasks

The aforementioned communication tools may have bits and pieces that allow companies to collaborate on projects, but for a more comprehensive strategy, organizations are deploying toolsets specifically for managing projects.

The caution with project management tools is like that of communication tools: Make sure that you aren't contributing to further siloing of information — content, documents and files. It's easy for knowledge workers to collaborate, have conversations, send documents back and forth and then lose sight of which version is the most recent, which document is where and so on.



Security tools

The cost of a security breach can be devastating — not only in terms of fines and costs but irreparable damage to a firm's reputation. Companies and their IT departments must consider the security risks of a remote workforce in terms of information access, access to internal IT infrastructure, resource allocation and more. What this means, essentially, is that when a knowledge worker accesses information, applications or other data remotely, then the risk inherently grows.

A remote workforce could entail public internet, local networks and consumer-grade security systems — all of which can increase security risk. A few of the online threats that remote workers and their employers should be aware of include:

Unsecured WI-FI networks.

Most remote employees will work from home, where they can secure their Wi-Fi. But true flexibility means that some may occasionally work offsite at clients' locations or they may work from a public location like a coffee shop — where they have to use unsecured public Wi-Fi networks. These are leading spots for malevolent parties to spy on internet traffic and collect confidential information.

Using personal devices and networks.

Many workers use personal devices and home networks for work tasks — a phenomenon known as Bring Your Own Device (BYOD). These devices often lack the security built into business networks — such as strong antivirus software, customized firewalls, and automatic online backup tools. This heightens the risk of malware finding its way onto devices and work-related information being leaked.

Basic Security Protection

Antivirus software, firewalls, encryption for devices... these need to be double-checked to ensure that security protection is active and up to date. Urge teams to upgrade their security software to the most recent version supported under the company's security policy and activate automatic updating on all company devices.

Virtual Private Network (VPN) Access

One way to secure information as it moves around between core systems of record and remote knowledge workers is to deploy a VPN. They provide a layer of security, which offers the following:

> Encrypting information transfers in transit
>
> Hiding users' IP addresses
>
> Masking users' locations

Larger organizations already have a VPN service deployed and, to scale a larger remote workforce, should verify they have adequate seats to provide this protection companywide. Firms should ensure that all remote employees are provided VPN access and that they use it for business-related activity.

Secure, Approved Cloud Services

One way to protect your employee end points is to ensure company information is not stored locally. Document storage should be cloud-based, and knowledge workers should be encouraged to use cloud-based apps.

It's also important that any third-party cloud storage services used — like Box, Dropbox, Google Drive and other file-shares — are verified for use by your security teams. Most of the tools we have listed for communication and collaboration, offer indeed some kind of integration to common cloud archives. But leaving this to the discretion of employees might be dangerous. With no direct involvement of IT, people might connect unofficial and personal accounts to company tools, exponentially increasing the risk for information leaks and data loss.

Information management tools

Have you ever opened your laptop in a coffee shop and suddenly realized the document you had to review is stored on your office workstation? Or have you ever had to take an important call with a customer from home just to find that you have three different versions of the contract, with different notes from different people?

It might not come as a surprise how important information flow is for employees to do their jobs seamlessly and efficiently remotely. For a truly flexible workplace, knowledge workers need anytime, anywhere access to up-to-date information. No matter where it is stored.

Companies have already triaged and implemented quick fixes (Box, Dropbox, Google Drive), but as time passes those solutions are found to lack the comprehensiveness needed to support a cohesive remote information management strategy.

For one, they require in most instances massive migration of data from other archives (ERP, CRM, network folders, etc.), and that is expensive and time consuming. As a result, employees often end up copying a bunch of files they need right away, creating duplicates and adding to the information sprawl that is familiar to many organizations.

Quick fixes also often lack the possibility to manage document lifecycle automatically, further burdening employees with manual and repetitive work. Whether it is a simple **DRAFT -> APPROVE -> SIGN** process, or a regulated retention procedure, that's not something you want to leave to the capacity of individuals to manually take the right action at the right time — particularly with the inevitable distractions that working remotely entails.

For these reasons, a more strategic alternative to those quick fixes is an intelligent information management solution.

There are three key characteristics that make intelligent information management a critical cornerstone of remote work, both in times of crisis and when business is carried out as usual.

Access to ALL information needed. The solution needs to connect to all organizational archives (ERP, CRM, network folders, content management systems, departmental tools, etc.) to give users a truly full picture of what is going on at any time.

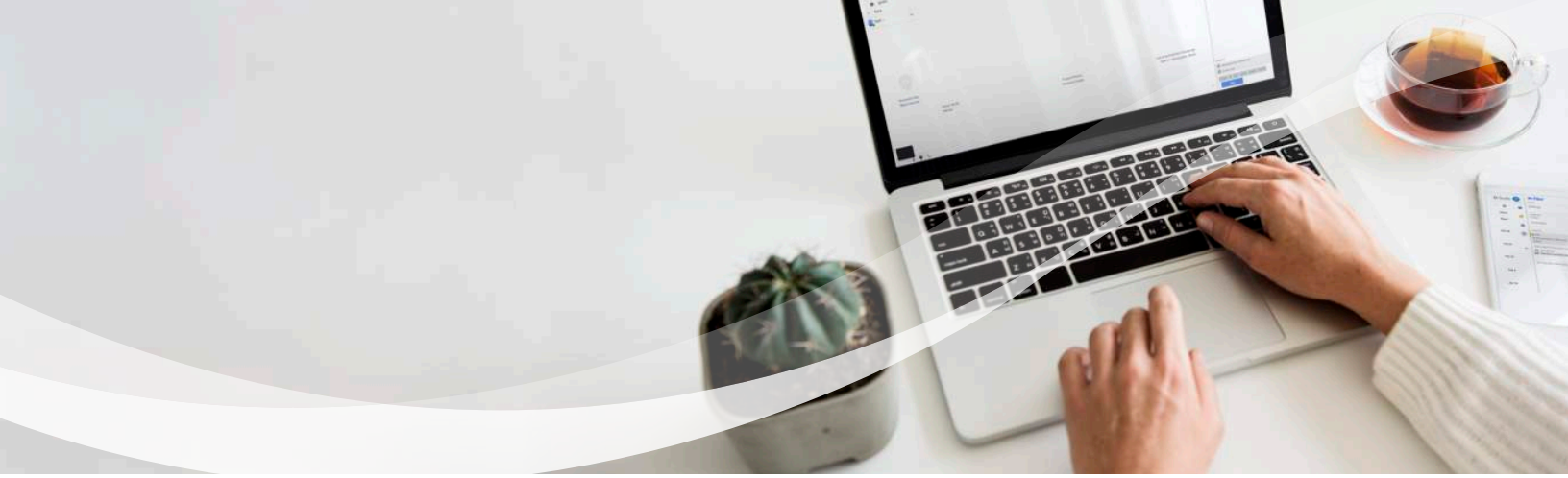
Information found IN CONTEXT. This means eliminating the need to search folders and sub-folders (and sub-sub-folders) to find the document the employee needs. Intelligent information management solutions enable people to always see up-to-date information that is relevant to their work.

AUTOMATED document lifecycle. Instead of having people from home pinging their colleagues to get drafts reviewed and plans approved, tedious and manual tasks can be automated with workflows, assignments and notifications. Employees can then focus on work that delivers value and deadlines are met with more consistency.

Knowledge workers working remotely need anytime, anywhere access to up-to-date information. No matter where it is stored.



M-Files



Closing thoughts

While the most recent events have forced many of us to work from home, a mobile workforce is an underlying trend that most companies have experienced, to at least some extent, for years now.

Whether it is to respond to a pandemic or to match the requests of the modern employee, organizations need to prepare for remote work with intention and strategy.

We believe the single most important decision to make is around the tool used to manage information. Business is largely contained in information — documents, files, images, videos, PowerPoint slide decks, Excel spreadsheets, and more. How information is created, categorized, stored and accessed will have a major impact on all other technologies your company is going to use to allow remote and flexible work. Some examples.

Communication. Workers that talk about and take decisions based on wrong or outdated information hurt businesses. When a single source of truth — a single copy of each document — isn't the standard, versioning issues and document sprawl are just the tip of the iceberg. What if, instead, documents could be shared while still ensuring they do not get duplicated or lost?

Collaboration. As documents are one of the most common and concrete manifestations of group work (plans, contracts, invoices), they are often touched by different people, who are supposed to take action and move on. This usually involves a lot of back-and-forth:

> "Have you checked the document I sent three days ago?"
>
> "Will you please sign off the invoice so we can pay it?"
>
> What if, instead, documents moved from one state to the next automatically, with people who are supposed to act receiving a notification or an assignment?

Security. Even with all the proper tools in place to ensure a basic level of security, the risk for sensitive information to be leaked when people work remotely is simply higher. This often happens because the general idea is that security stifles productivity. And so, when faced with the trade-off between the two, companies often forgo the former in favor of the latter. What if, instead, security was built-in to how information is managed and shared, with sensitive data automatically identified and access restricted based on roles, groups or even user IDs?

With an intelligent information management platform, the key principles that underpin a solid flexible work strategy are already there. All you have to do to work remotely is grab your laptop and go. The information, files and documents needed are a couple of clicks away, accessible from any device. It's this concept of anytime, anywhere access to company information — with a built-in information security framework — that truly sets the stage for remote working, giving staffers the same experience as they would have at the office.

And by doing that, companies can ensure continuity, productivity and efficiency of their remote, modern workforce.

M-Files

About M-Files

M-Files provides a next-generation intelligent information management platform that improves business performance by helping people find and use information more effectively. Unlike traditional enterprise content management (ECM) systems or content services platforms, M-Files unifies systems, data and content across the organization without disturbing existing systems and processes or requiring data migration. Using artificial intelligence (AI) technologies in its unique Intelligent Metadata Layer, M-Files breaks down silos by delivering an in-context experience for accessing and leveraging information that resides in any system and repository, including network folders, SharePoint, file sharing services, ECM systems, CRM, ERP and other business systems and repositories. Thousands of organizations in more than 100 countries use M-Files for managing their business information and processes, including NBC Universal, OMV, Rovio, SAS Institute and thyssenkrupp.

For more information, visit **www.m-files.com**.

M-Files has offices in eight countries. To contact one of our regional offices, click here: **www.M-Files.com/en/contact-us**.

M-Files is a registered trademark of M-Files Corporation. All other registered trademarks belong to their respective owners.



linkedin.com/company/m-files-corporation



@M _ Files

M-Files