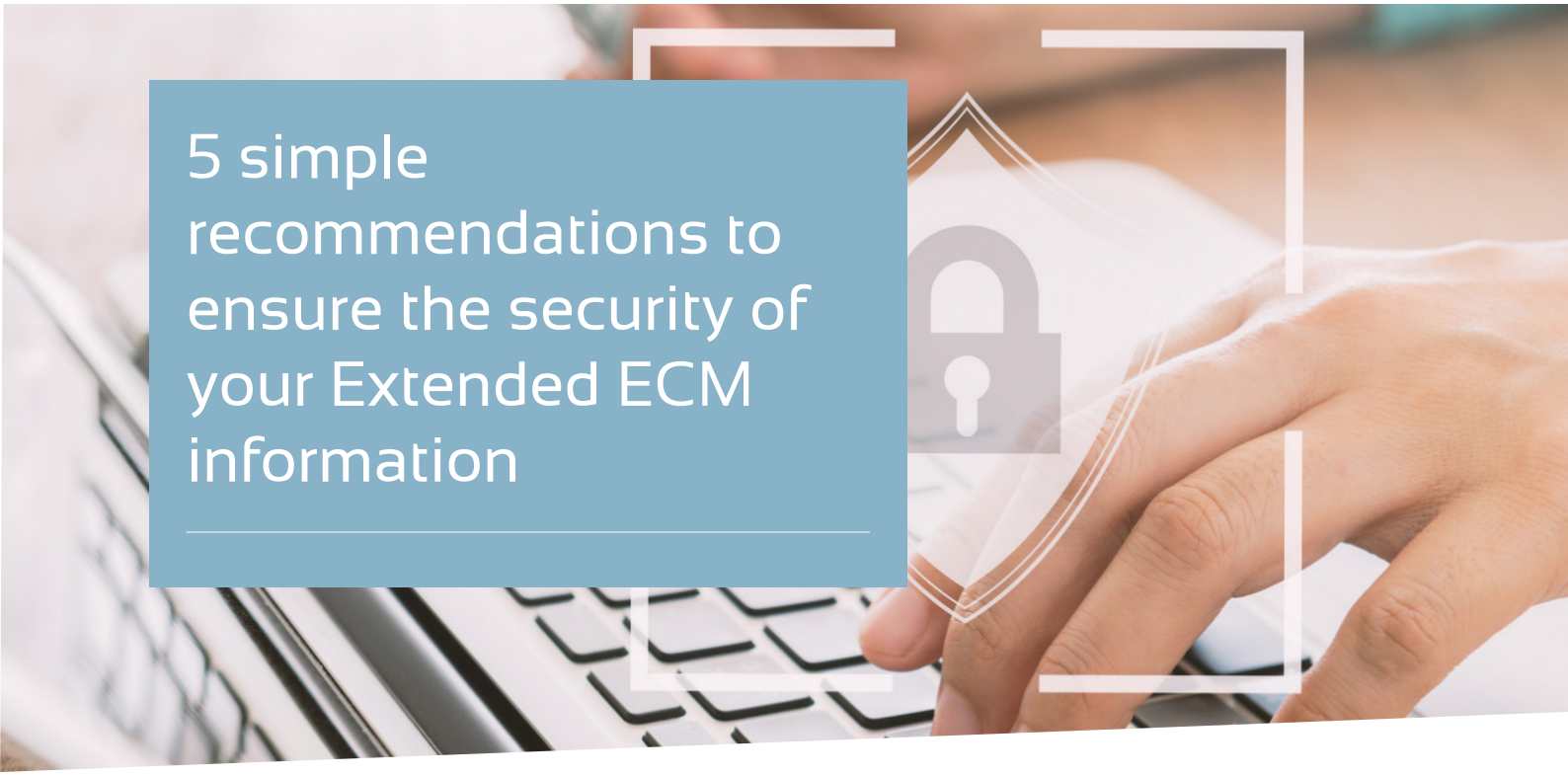
Fastman



5 simple recommendations to ensure the security of your Extended ECM information

So many organizations are ruined by insecure data. Without confidence in your data, you can't make secure decisions and run into confusion at every step of your operation. If you want to streamline your operations and increase productivity, it all begins with information security. The catch? It can seem difficult to do it yourself! We found that solid information security all comes down to five essential recommendations that we've made to our clients' countless times for their success.

Let's get into it.

The importance of information security

Information security is about process and control - running parallel with cyber security instead of within the same scope. Where cyber security focuses on the network and prevention of infrastructure-based attacks, information security is the prevention of data-specific risks.

Companies that use enterprise content management (ECM) platforms rely on information security measures like permissions management. Without the implementation of basic security measures, companies run the risk of losing their reputation, competitive advantage and opening their company up for easy attacks.

Information security is essential, especially in the digital age, because data can make or break a company if it ends up in the wrong hands. Beyond this, it is imperative to ensure that the right people are working with the right data to maintain structure and better production value - but also so that important data doesn't get lost.

Many organizations struggle to get these elements to work in tandem when in reality, it can be quite simple to ensure your data integrity. Below, we'll outline five ways you can ensure data integrity for your own ECM platform- whether it be OpenText, SAP or something else.

Five recommendations to ensure data integrity

Assign permissions

Permissions management is a security measure that manages what data, features and end-users are permitted access. Good permissions management sees users that are only allowed access to data and tools that they need for their specific tasks.

By using permissions management and assigning permissions where necessary, organizations can benefit from tighter security, reduced risk, greater data control and fewer errors. A permissions management solution thus allows data administrators to take control over their ECM system - which inevitably boosts information security.

We found that 28% of respondents cited well-defined access control and permissions provided the most effective business information protection method.

Regularly manage your access control

As an add-on to permissions access, managing your access control refers to updating who is allowed to access certain information and on what devices. This becomes particularly challenging with the recent move to more remote work, as employees might need access to information from their personal devices.

In today's work environment, employees will be able to access more sensitive information from their personal devices - both on the clock and off. This poses a risk for companies, and more data security measures will be necessary to protect information. Effective access control while regularly updating permissions is the solution for companies who want to remain flexible but stay secure.

Conduct internal audits

Detective mechanisms are useful to identify where your security risks are stemming from. When speaking to respondents, 67% used a combination of detective measures to identify risks within their company. This sees a need for a multifaceted approach that uses good processes and strong tools to ensure the integrity of business data.

However, 44% of respondents used their own security audits to detect these issues. This is a big indication that organizations and businesses feel more comfortable using their own resources - and as such, are likely using internal security and permission evaluation tools. This speaks to the need for companies and organizations to invest in excellent security measures and audit systems that use the best processes to identify security risks within the company.

Ultimately, internal audits help tighten your security and assist you with finding holes in your objectives and policy that would otherwise go unnoticed until it's too late. This makes it a critical addition to ensuring your ECM security is secure and up to date.

Optimize manual processes

Automating manual processes has often been touted as the best way to ensure more production value and fewer errors – but the key is not in automation, but efficiency.

When it comes to information security, the last thing you want to do is lose control – whether that be to automated bots or humans. Instead, optimized processes help you stay in control and lead to a state of meaningful and effective security without sacrificing productivity. Tools that give administrators the option to quickly locate security risks and bulk update permissions mean that info security processes become less time consuming, and more secure without resorting to automation.

Effectively dispose of unneeded documents

Stray and obsolete documents create clutter and confusion while introducing security risks for your entire organization. However, as more digital documents are created and propagated, it is not as easy as merely shredding unnecessary pieces of paper. In many ECMs, destroying or deleting documents does not always mean they are eliminated from the system entirely. Using the wrong procedure or method can cause copies of the document or backed-up versions may exist elsewhere, accessible by other users once forgotten.

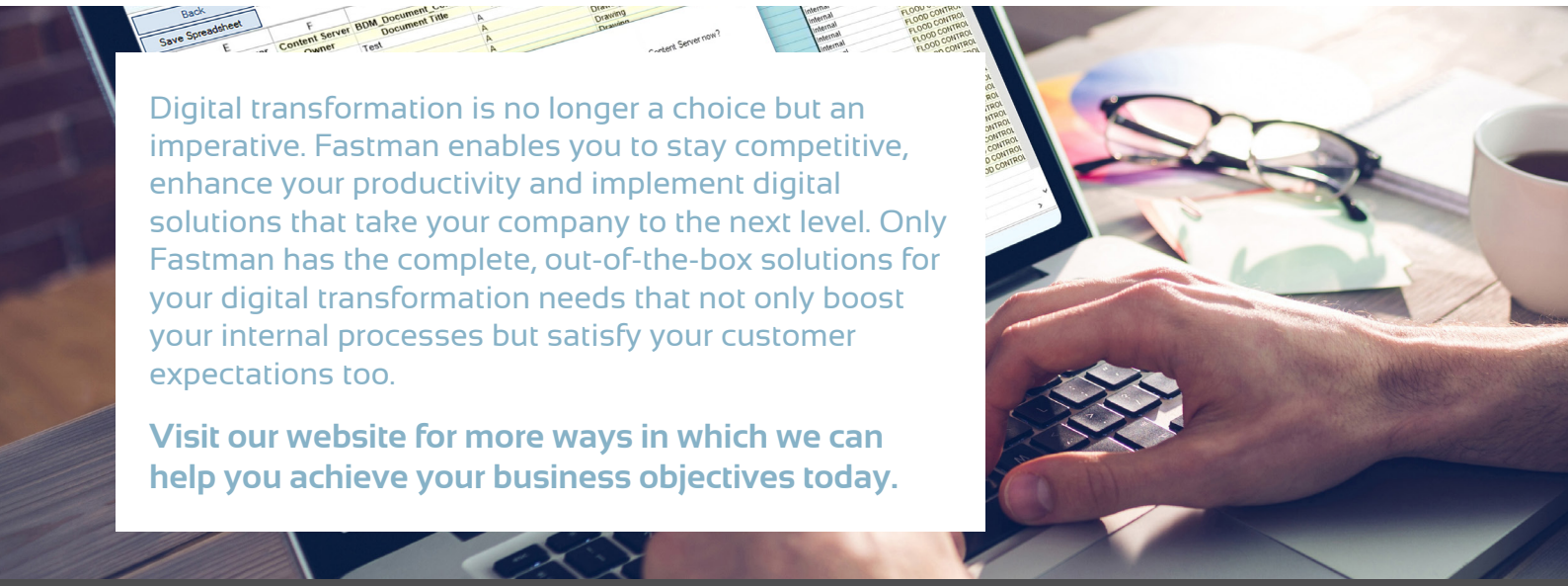
Instead, strategically archiving documents and having a strategy to determine which documents need to be safely destroyed will help reduce clutter and increase security throughout the company. Employees will no longer need to dig through files to find the piece of information they need, and companies will be able to completely control access to their data.

Implementing your solutions

Managing information access control and solutions can be a challenging task. However, especially in the digital age, it is essential to ensure that your information is protected in the best way you know possible.

However, we understand that many people may not have the expertise or tools to implement effective information security themselves. It can take months, or even years to get it right - and most organizations just don't have the time, leaving their data at risk and their processes in disarray.

Fastman has worked on effective solutions for these problems for a long time, with many companies. By providing the tools you need for effective information security, Fastman are Content Suite and ECM experts that provide solutions for both OpenText and SAP. Contact us today to find out how you can best protect yourself. Arrange a meeting; we will review your information handling processes and provide steps to ensure integrity. Implement the change; we will provide concise recommendations that will ensure the integrity of your information. Trust your content; with technology and processes in place, you can trust the integrity of your platform and the information within.



Digital transformation is no longer a choice but an imperative. Fastman enables you to stay competitive, enhance your productivity and implement digital solutions that take your company to the next level. Only Fastman has the complete, out-of-the-box solutions for your digital transformation needs that not only boost your internal processes but satisfy your customer expectations too.

Visit our website for more ways in which we can help you achieve your business objectives today.

(NA) +1 (949) 955-4949
(AU) +61 3 9804 8251
(SG) +65 6679 5686
(NL) +31 6 4206 3775

www.fastman.com
info@fastman.com

Fastman