



Keep the ownership of your documents

Why is it so important?



We find every day in the workplace situations where we need to ensure that certain documents are under control. They have important information that if it goes to the wrong hands it could cause us trouble. We would like to make sure that even IT staff could not access them. Wouldn't it be great if we could keep our critical documents under control?

The information contained in this document is confidential and proprietary to SealPath Technologies SL. No part of this document may be distributed, used or reproduced without the prior written consent of a representative of SealPath Technologies SL.

Why do I need to keep my documents under control?

"I want to control the risk of having our critical documents spread in different locations and devices and... finally reach the wrong person by mistake"

Ann Harrison, CEO, Manufacturing Company – Automotive Sector



"We usually work with critical documentation regarding components specification, new prototypes, and specific requests from manufacturers, which we need to keep under control. We have invested too many hours of work and money in some of our projects that I wouldn't like to see how we lose our leadership and advantages due to errors related to how we manage our corporate information. We need our technical and engineering staff work with the information at home or on laptops outside the company to close projects on time. It is a matter of productivity. But I also want to control the risk of having our critical documents spread in different locations and devices and... finally reach the wrong person by mistake".

"A Solution for our problem is to be able to **decide who has access to the corporate documentation no matter wherever it is**. Be able to revoke permissions over the documents in real time to the one that should not access them even if the documents are in his hands, and be able to keep control over every copy of the documentation in any place"

"... An employee sent an Excel spreadsheet with hidden columns that contained data about salary and other confidential information to everybody in the company"

James Blake, Human Resources, Investment Banking

"In our department we work with confidential data from employees that are protected by different data privacy regulations. Apart from this, we must have special care keeping the privacy of personal data".

"Some months ago, we had a new employee in the department that shared on request the phone numbers, email addresses and role of every employee with a manager of subsidiary. She thought that it was a good idea that this information could be available to everybody in the company so she sent the document to everyone in the company. The intention was good but after some weeks we knew that the spreadsheet went out of the company and some executives were receiving uncomfortable calls".



"It could be even worse. One friend told me that in his company an employee sent an Excel spreadsheet with hidden columns that contained data about salary and other confidential information to everybody in the company."

"It would have been great if we could have given permissions only to employees to access to this documentation, and even, be able to remove it remotely in case of detecting any problem".

“Our partners should have access our information for a limited time period, but after this, we should be able to revoke permissions over it”

Eduard McLean, Project Manager, Civil Engineering



“We work in engineering projects that while they are active we have to exchange critical information with our project partners. In some way, we are giving our know-how to these partners depending on the type of information we exchange with them.”

“The problem is that, one company can be your partner in one project, but once this has finished, the same company can be your competitor in another one. Sometimes we go together to a tender and sometimes we go with other partners”.

“We should be able to give permissions over the documentation we send to these partners just for the time the project is active, but once finished, **this documentation should be automatically destroyed**, due to it is not information owned by the partner”.

“Since Dropbox is used, the data leakage problems are rocketing”

James Oldfield, Chief Information Officer, Law Firm

“Dropbox has become so popular among our corporate users that it is now one of the most common document sharing channels. We have an FTP and a Document Management system to share documentation with third parties, but finally Dropbox is with difference the most used sharing tool”

“Now we have documentation going out of the company without any control regarding who is sending it out, the receptors, etc. With Dropbox, the data leakage problems are rocketing”.

“Due to productivity reasons, we need that our users share the information through the most comfortable for them, but we need that the confidential or critical information travels always protected and remains under control. This kind of documentation must be protected in order only people authorized access to them and we can always audit who is opening it”.



"We need to control and audit who can access to information related to our patients, clinical data, etc."

Mary Reims, Organization and Risk Assessment Department, Private Health Center



"Health related data are one of the types of data where the law is stricter trying to guarantee that they stored carefully and maintaining the highest standards of privacy. We need to control and audit who can access to information related to our patients, clinical data, etc."

"From our point of view it is not difficult to control the access to the structured information we have in our databases used by our management applications. People access with their credentials, and only see the information they can with their privilege level".

"The problem comes with the *unstructured* data we have in documents created by internal users or exported from our management applications. It is absolutely critical to be able to guarantee that these documents are **encrypted and under control, and that no matter where they are located only authorized people can access to them**. We need also to know who is trying to access to them without permissions and keep a complete audit trail of access to the protected documents.

"Contractors must only have access to the documentation for a limited time period"

Dorothy Lewis, Product Development Director, Aerospace sector

"We usually cover Production peaks with the help of outsourcing and contractors very specialized in our sector. The external staff works for some months like if they were part of our permanent staff. The problem is that once they leave our company they can start working for other companies that can be competitors".

"The contractors must only have access to the documentation for a limited time period. Of course, once they have left our company, we should be sure that they not take our documentation with them that at the end can go to the competition"

"It would be needed to guarantee that **they only can access to the documentation while they are working with us, but once out they lose access to our corporate documentation"**



What can we do to keep the ownership and control over our documents even after sharing them?

SealPath allow you to set permissions over the documents so that only you decide who will be able to access to the documentation wherever it is. It also allows you to set expiration dates over the documents, and once that this date expires the people you decide will lose access to the documentation.



The documents always travel with the protection and are encrypted. It is a persistent protection that only who has applied it can remove it. You can change in real time who has access to the document, revoke permissions by remote or even “destroy” the documents remotely.

It also allows you to monitor who and when is accessing to the documentation, who from outside your company has access to the protected documents no matter where they are, etc.

SealPath covers your needs of confidential documentation protection and control being able to keep your most valuable documentation safe from data leakage.



SealPath protects your critical and confidential documents, and allows you to keep them under control wherever they are

|  Information Protection |  Use Control |  Audit and Monitoring |
|--|---|--|
| Your corporate documents secure and encrypted wherever they are | Decide who can access and the level of permissions (view, edit, print, copy&paste, etc.). Destroy documents remotely. | Control in real time actions over the documents. Monitor who is accessing, blocked accesses, etc. |