

APF Information Protection and Access Control (IPAC) Solution

User Case and Design for Law Firms

Law firms handle most sensitive information for their clients, despite swearing an oath and does their best protecting their clients' best interest in the courts, the same can't be said for the effort to protect client information from cyber attack as well internal breach of trust. Last year two of the largest firms in the United States, Cravath, Swaine & Moore and Weil Gotshal & Manges, , got caught in a major cybersecurity breach later linked to a \$4 million-plus insider-trading scheme (more cases can be [found here](#)). This is more than just a technology issue or an added clause in the retainer agreement—it's the biggest risk that law firms face today. Clients also see this as a big risk: according to the 2016 ABA *Legal Technology Survey Report*, 30.7 percent of all law firms and 62.8 percent of firms of 500 lawyers or more reported that current or potential clients provided them with security requirement, demanding that the firm has detailed cyber-security plans and prevention tools.

APF Technologies meets the challenge head-on with the latest Information Protection and Access Control (IPAC) solution. Besides guaranteed information protection at all times, IPAC also contains features that are specifically designed to work with all law firms - no matter how large - to meet even the most stringent of security demands by any client.

Protection for every document anywhere at all time

With IPAC, documents are protected by the strongest encryption at all time no matter if they are stored on backend servers, cloud storage, personal laptops or mobile devices. No documents will be stored plainly - anywhere.

Rest assured, IPAC's protection doesn't compromise productivity and the information flow. The protected document can be shared through email, shared cloud storage. Although document flow remains the same, the access to the content, however, is subject to IPAC's access control to further limit the exposure of the information.

Trusted but Verified

Since law firms are built on reputation, internal security breach can be just as devastating as external ones. IPAC's access control allow the information access align with firm-wide governing policies, permitting the information from one client to be accessed only by the personal who is currently works with client and no one else. When attorneys get reassigned to different cases, their permission will change accordingly and take effect immediately on all the copies of the previous client's files - regardless where the files are being stored, even those on personal laptops or mobile devices. With IPAC, firm can effectively build an electric wall between the teams for conflicting clients to ensure there is no document sharing.

IPAC also eliminated the need for non-client team to access client's information, further reduce the risk of breach. Until now, some supporting teams including IT, with their application and infrastructure admin access, were inexplicitly given the access so they can managing system that stores the documents. IPAC's

advanced design separating the access to the documents and contents removes that risk. IPAC doesn't give admin the access to the contents beyond the firm access policies while maintains their access to the files.

Document life cycle management

In today's connected world, managing documents life cycle is challenging as ever. Documents can easily be shared, copied and stored anywhere, so to truly remove a time sensitive document is a difficult task if possible. IPAC provide 2 ways to handle the task properly. First, it allows access policies to temporally disable access to the content after a set date. Reversing the policy would reverse the access control and allow the documents to be viewed again. Second, IPAC digit "shred" the document to permanently prevent the content of the document to be accessed, regardless of the number and location of the copies exists.

Audit Records

With IPAC, every access to the documents and every change that could impact the access of the documents are recorded and audited. Externally, this provide the firm with the data to confidently satisfy client's demand to audit the access of their information. The data is feed into advanced artificial intelligence analytic tool to detect early signs of possible breaches so preventive measures can be taken internally, as well as to better understand the team performance.

Meta data management

IPAC protects the contents of document so those document will not be exposed to any internal search engine, which is potentially security volatility. To make the protected document reachable, IPAC provide effective Meta data management for the protected document. The Meta data of protected document has a description, tag and version, so the protected documents can be categorized and searchable.

IPAC is the cyber security solution that gives the firm the confidence of knowing their information and reputation are being protected to their best capability and no less.