Six Stages of Document Security

Data Conversion Specialist

6 Stages of Document Security: Protecting Paper & Electronic Documents

A modern business processes a great deal of information but often doesn't have proper visibility of how it is produced, stored, and accessed, leading to potential security flaws. Here we look at the six stages of Document Security you need to consider when developing a Document Security Policy to protect your paper and electronic documents.

Many organizations process thousands of documents daily, in all types of formats, and every day they are in danger of being lost, stolen, or compromised. Regardless of your business's size, protection and the security of your documents is an important requirement for the security of your company.

Industry analyst **I**nternational **D**ata **C**orporation (IDC) predicts that worldwide data creation will grow to an enormous 163 zettabytes (ZB) by 2025. That's ten times the amount of data produced just a couple of years ago.

The volume, complexity, and diversity of information a business creates and consumes leads to document management and control challenges. To overcome this challenge, a company must understand and map document types - how they are used, how they interact with business processes, how they are stored, managed, distributed, and preserved.

The definition of Document Security (or lack of it) is a very broad topic. It needs to be considered from the document lifecycle perspective, especially concerning:

- Data breaches
- Unstructured data
- Unsecured files
- Human error
- Unauthorized access to storage

We define document security as security related to information captured from paper documents through the scanning process or digital documents stored in business repositories, for example, Microsoft Office files or emails.

We believe there are six main stages to a document's life.

Stage 1: Capture

Capture is the process stage that describes the 'on-boarding' of information, whether that is the scanning of hard-copy documents, monitoring a 'watched' email 'inbox' or creating and saving documents from an application.

Scanning is the most common way of transferring hard copy content to electronic formats. But while convenient, unless controls are in place, the process is not traceable, which can lead to security and legal admissibility challenges. For example, a document can be scanned but what then happens to the original hard copy version.

Routing is the process used to send captured documents to the correct storage location. Without document routing, the possibility that a document may inadvertently be stored in an incorrect or even unsecured location is real.

Stage 2: Store

Secure storage can be paper-based or an electronic file system, but many companies overlook the storage type, location, and security required. if paper based then security also may related to the conditions of the storage environment. Is the humidity too high? Are documents protected against mildew? What about fireproofing or automated fire control (such a sprinklers).?

Paper-based storage systems are still widespread but often lack the required security controls. Also, it is challenging to show any audit information related to paper documents.

Electronic based storage is often implemented with the expectation that it is a better way. Still, without appropriate design and management, this creates challenges. For example, how the data management system needs to be protected within the business network. Access rights need to be defined and set up. The system also needs to be monitored for unrestricted use.

Stage 3: Document Management

Management concerns the permissions, the user roles, version control, and Audit trails. Permissions are used to manage users' access rights to documents, so they are vital in maintaining a secure document environment.

While permissions are often easy to understand, they can be challenging to introduce and manage without the right systems. To effectively implement permissions, the business must first understand how users' activity relates to the information they must access and their involvement processes.

Audit trail stores records of every activity and transaction applied to a document, for example, who created, modified, viewed, or re-versioned. Audit trails provide the ability to prove activity relating to all documents stored and are key to maintaining security, particularly when a data breach occurs.

Stage 4: Preserve

Preserving documents and information – document retention – is another key aspect of ensuring a secure document environment. However, documents stored in traditional or electronic repositories require constant maintenance as the available space is limited.

Some documents should be kept (by law) for a certain number of years. The challenges in doing so include:

- Maintaining a record to ensure only documents beyond the retention period are removed.
- Ensuring that all versions of the documents under the retention policy are accounted for.
- Deciding whether users should manage their libraries or whether the process should be managed centrally.

Next, businesses need to set policies to securely dispose of all paper information, electronic files, and electronic libraries once they are out of date or the retention period has expired, via physical and electronic shredding.

Stage 5: Access and Sharing

The Deliver stage defines how an electronic document can be shared with other users or business partners.

Document sharing is frequently done by using shared folders or drives, but if not managed correctly, this can lead to the files being found, accessed, and used by unauthorized users or user groups.

Accessing documents through mobile devices can also be part of the delivery stage, bringing more complex issues to securing the access.

Stage 6: Integration

Integration is the process used to exchange information with other business applications, for example, an accounting or ERP system. For integration to be successful, all the preceding stages are critical to providing consistent and accurate data.

The Solution

Document Security is one of the most critical aspects of security in every business. Unfortunately, building a Document Security Policy can be a time consuming and complicated process.

Use a proven approach to Document Security. Use a consultant that knows and can guide your company through the process and help you defined options and determine the optimal strategy. The consultant you select needs to be up to date with the latest security regulations and general data protection regulations.