5 Security Best Practices for Contract Management

A new post from **Contract Logix** offers some advice on how to avoid landing in a nightmare business situation: Imagine if a disgruntled employee or ambitious hacker accessed the details of your most important and sensitive contractual agreements and did something malicious with the information. Just think about the potential legal, financial, and brand liability.

Security breaches like this can result in the most severe and highest profile consequences for your business, especially in today's hyper-connected world of social media. Unfortunately, the contracts at many organizations are scattered throughout the company in file cabinets, on individuals' hard drives, or in shared folders – exposing the business to significant risk.

Below are 5 security-focused best practices you can implement to better protect your contracts:

1. Centralize all your contracts in a secure electronic repository.

It's not uncommon for organizations to store contracts in shared folders across multiple locations and formats. However, centralizing your agreements in a password protected and cloud-based repository is the most important step towards secure contract management. Not only will it keep your agreements organized, it greatly reduces the risk of them being accessed by the wrong individuals and stores them in a safe place. It also allows you to securely access any document at anytime from anywhere on any device.

2. Implement role-based security to your contracts and related information.

Another challenge with storing contracts in multiple places is that it’s impossible to govern tiers of access to them. Once you’ve centralized your contracts online, you’ll be able to set role-based permissions for enhanced security. This allows someone to read or write certain document or contract types but denies them access to others that would be inappropriate to edit. It also prevents unauthorized users from seeing or editing contract details.

3. Ensure all your contract data is encrypted in transit and at rest.

An important best practice to protect your contracts from unauthorized users is to encrypt all your document data. You’ll want to encrypt information both at rest and in transit using the latest AES 256-bit encryption and TLS 1.2 standards. Data at rest refers to any data that is stored within your contract management system. Data in transit refers to any data that is being sent externally to or from your contract management system to a user or another application.

4. Leverage E-signature capabilities.

The most time-consuming part of any contract process is getting approvals, especially for those chasing down paper-based signatures. E-signatures are a best practice to get documents signed faster. More importantly, however, is that e-signatures are more secure than paper ones. They have been legally binding for over 15 years thanks to the ESIGN Act of 2002. E-signatures carry a digital record about who, when, and where a document was signed to ensure authentication and help with audit trails. Be sure to fully capitalize on the benefits E-signatures offer your organization.

5. Intake your contract data through secure forms.

Many organizations still rely on email to request contracts and capture required data to create them. This often leads to incomplete or incorrect information which adds time and

creates risk. Email attachments are also the most common way hackers infiltrate corporate networks with malicious software. With pre-defined and encrypted intake forms, team members can quickly and accurately submit an existing contract, request the creation of a contract, or if they have the authority, instantly create a contract. This ensures the integrity and security of data captured for your contracts, eliminates the need for double data entry or chasing down missing data, and minimizes mistakes.

Takeaway

The number of security breaches and malicious hacks continues to skyrocket. Given that contracts are the backbone of your business, you can increase the security of them by implementing these five best practices. Not only will you have greater piece of mind, you'll also avoid potential financial, legal, and brand risks.