Foxit

Do More with Documents

Securing the Document Lifecycle

A Practical Guide for IT Leaders Building Secure Document Workflows

How to protect sensitive information, maintain compliance, and reduce risk across the document lifecycle

Table of Contents

Documents are the lifeblood of business operations. Contracts, financial records, customer data, employee information, compliance documentation, and intellectual property all exist as documents that must be created, shared, reviewed, approved, and stored. These documents are also prime targets for security failures—and the consequences of getting security wrong are significant.

Most organizations lack a unified approach to document security. Encryption practices vary by department. Access permissions are inconsistently defined and enforced. Employees use unvetted tools to convert, share, and sign documents. Version control is haphazard, with multiple drafts circulating across email threads and shared folders. The result is a fragmented security posture with gaps that put sensitive information at risk.

The cost of these gaps is not abstract. Data breaches carry an average global cost of $4.35 million, with US incidents averaging $9.44 million. Beyond direct financial impact, organizations face regulatory fines, legal liability, customer churn, and reputational damage that can take years to repair.

This white paper is designed for IT leaders, security professionals, compliance officers, and operations leaders who need to strengthen document security without slowing their teams down. You will learn how to assess your current workflows, implement practical security controls at each stage of the document lifecycle, evaluate solutions, and build a document management approach that protects sensitive information while enabling efficient collaboration.

The goal is straightforward: help you take control of your documents so you can reduce risk, maintain compliance, and give your organization peace of mind.

The Problem: Documents Are Everywhere, Security Is Fragmented

Every department in your organization creates, shares, and stores documents. Finance handles invoices, budgets, and financial statements. Legal manages contracts, agreements, and compliance records. HR processes offer letters, performance reviews, and employee files. Sales produces proposals, quotes, and customer communications. Operations documents procedures, training materials, and project plans.

Each of these departments often uses different tools and follows different practices. Some encrypt sensitive files; others do not. Some use approved software; others rely on whatever free tool they find online. Some maintain strict version control; others circulate multiple drafts with no clear source of truth.

The shift to remote and hybrid work has expanded the attack surface further. Documents now move across home networks, personal devices, cloud storage services, and collaboration platforms. The traditional security perimeter—if it ever truly existed—has dissolved.

Common security gaps include:

- **Vague or undefined access permissions:** Who can view, edit, or share sensitive documents? In many organizations, the answer is unclear—or everyone.
- **Inconsistent encryption practices:** Some documents are encrypted; most are not. There is no standard policy or enforcement mechanism.
- **No version control:** Multiple drafts circulate with no clear indication of which is current or approved. Changes go untracked.
- **Undefined archiving and backup:** Documents are stored inconsistently. Some are backed up; others exist only on individual devices or email accounts.

- **Shadow IT for document handling:** Employees use unapproved tools—free online converters, personal cloud storage, consumer-grade signing apps—to get their work done.

IT and security teams are accountable for protecting sensitive data. But when document workflows are fragmented across departments, tools, and locations, that accountability becomes nearly impossible to fulfill. You cannot secure what you cannot see—and in most organizations, document handling is largely invisible to IT.

The Cost of Getting It Wrong

Document security failures carry real financial consequences. According to IBM Security research, the average global cost of a data breach reached $4.35 million in 2022. In the United States, the average cost was significantly higher at $9.44 million. These figures include direct costs like investigation, remediation, and notification, as well as indirect costs like lost business and diminished customer trust.

Beyond the immediate financial impact, organizations face additional consequences:

- **Regulatory fines:** GDPR violations can result in penalties up to 4% of global annual revenue. HIPAA violations carry fines up to $1.5 million per incident category. Industry-specific regulations add further exposure.
- **Legal liability:** Improperly secured documents can lead to lawsuits from affected customers, partners, or employees. Contract disputes may arise from unsigned, improperly signed, or tampered documents.

- **Customer churn:** Customers who lose trust after a security incident take their business elsewhere. Rebuilding that trust—if possible at all—takes years.
- **Reputational damage:** News of data breaches spreads quickly. The association between your organization and compromised security lingers in search results and public memory.

Consider how easily document security can fail in practice:

- A sensitive contract is emailed without encryption. It is intercepted, forwarded, or accessed by unintended recipients.
- An employee uploads HR documents to a free online converter. The service retains copies, exposes them through a security flaw, or sells the data.
- A document is signed using an insecure method. Its validity is later challenged in legal proceedings, and the organization cannot prove authenticity.
- A former employee retains access to confidential files because permission controls were never properly defined or revoked.

Document security is not just an IT concern—it is a business risk that affects finance, legal, HR, operations, and customer relationships. The cost of prevention is a fraction of the cost of remediation.

What Is a Document Management System?

A document management system (DMS) is a framework of tools and processes for creating, storing, organizing, securing, and retrieving documents digitally. It provides visibility into how documents move through workflows, who has access, and how files are reviewed and updated over time.

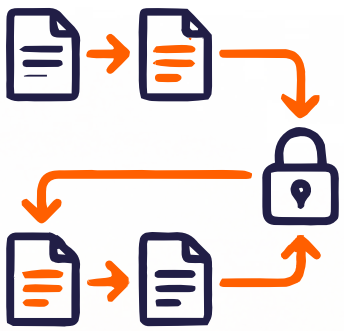
Core capabilities of a document management system include:

- **Indexing and search:** Documents are tagged with metadata—file names, dates, categories, descriptions—making them easy to locate and organize.
- **Access permissions and authentication:** Controls define who can view, edit, or share documents, with authentication ensuring users are who they claim to be.
- **Version control and audit trails:** Changes are tracked, creating a clear history of who modified what and when.
- **Encryption and security controls:** Documents are protected at rest and in transit, with options for password protection, redaction, and digital signatures.
- **Collaboration and workflow routing:** Documents can be shared, reviewed, approved, and routed through defined processes.

A document management system replaces ad-hoc processes—email attachments, shared drives with unclear folder structures, paper files in cabinets—with structured, governable workflows. It provides the foundation for document security by making document handling visible, consistent, and controllable.

But a DMS alone is not enough. Security must be built into every stage of the document lifecycle—from creation through archiving. The following sections outline a practical framework for doing exactly that.

Building Secure Document Workflows: A Practical Framework



Secure document workflows are built on a series of practices applied consistently across the document lifecycle. No single feature or tool provides complete protection—security requires a layered approach that addresses how documents are created, shared, reviewed, signed, and stored.

The following seven steps provide a practical framework for strengthening document security:

1. **Assess your current document workflows** to understand how documents are handled today and identify gaps.
2. **Use PDFs as your security foundation** to leverage built-in encryption, permissions, and protection features.
3. **Control document versions** to ensure teams work from current files with clear change tracking.
4. **Apply password protection and encryption** to restrict access to authorized users.
5. **Redact sensitive information** to permanently remove confidential content before sharing.
6. **Sign documents securely** using eSignatures and digital signatures with authentication and audit trails.
7. **Digitize paper documents** to bring physical records into secure, searchable digital workflows.

Each of these steps is explored in detail in the following sections.

Step 1: Assess Your Current Document Workflows

Improving document security starts with understanding how documents are currently handled across your organization. Before implementing new controls, you need a clear picture of existing processes, tools, and gaps.

Audit your document workflows by asking:

- **How are documents created?** What tools do employees use? Are they approved and secure, or do teams rely on whatever is convenient?
- **Who has access to sensitive documents?** Are permissions defined, documented, and enforced? Do former employees or contractors still have access?
- **How are documents shared externally?** Email attachments? Cloud links with open access? USB drives? Each method carries different risks.
- **How are versions tracked?** Is there a single source of truth, or do multiple drafts circulate without clear indication of which is current?
- **What happens after projects end?** Are documents archived according to retention policies? Deleted when no longer needed? Or left in place indefinitely?
- **Where does shadow IT occur?** Are employees using unapproved tools—free online converters, personal cloud storage, consumer signing apps—because approved alternatives are unavailable or inconvenient?

Look for patterns that indicate risk: inconsistent practices across departments, paper-based processes that bypass digital controls, and workarounds that employees have developed because official tools don't meet their needs.

The output of this assessment should be a clear understanding of where your document workflows are strong, where gaps exist, and which improvements will have the greatest impact on security.

Step 2: Use PDFs as Your Security Foundation

PDF is the most widely used format for secure document sharing—and for good reason. The format preserves content and layout across systems, ensuring documents look and behave consistently regardless of where they are opened. More importantly, PDF includes built-in security capabilities that other formats lack.

Built-In Security Capabilities

PDFs support robust security features that give document owners control over how files can be accessed and used:

- **Permission controls:** Define who can view, edit, print, or copy content. Restrict actions to prevent unauthorized changes or distribution.
- **Encryption:** Convert document contents into unreadable data that requires a password or certificate to decrypt. Without proper credentials, the file cannot be accessed.
- **Content protection:** Guard against unauthorized modifications, ensuring the document's integrity is maintained throughout its lifecycle.

Content Security vs. Application Security

When working with PDFs, it's important to consider both content security and application security. Content security focuses on protecting what's inside the document—the text, images, and data. Application security focuses on protecting the software itself from vulnerabilities and misuse.

Keeping PDF software up to date is an essential part of maintaining a secure document environment. Updates often include security patches that address newly discovered vulnerabilities. Outdated software creates exposure that attackers can exploit.

PDF is not just a file format—it's a security framework when used properly. Tools like Foxit PDF Editor make it easy to encrypt, password-protect, and apply permission controls to PDFs as part of everyday workflows, ensuring security doesn't require extra steps or specialized knowledge.

Step 3: Control Document Versions

Document versioning ensures teams work from the most current file rather than outdated drafts circulating via email or scattered across shared folders. This is especially critical for complex documents that involve multiple contributors and review cycles—contracts, proposals, policies, and compliance records.

Without version control, confusion multiplies. Which draft is current? Were the legal team's changes incorporated? Did someone revert to an older version by mistake? These questions consume time and create risk when the wrong version is signed, submitted, or published.

How Automated Versioning Helps

Automated version control eliminates the need for manual file naming conventions like "Contract_v3_FINAL_revised2.pdf." Instead, the system tracks:

- **Who made changes:** Each edit is attributed to a specific user, creating accountability.
- **When changes occurred:** Timestamps document the evolution of the file over time.
- **What was modified:** Specific changes can be reviewed, compared, and if necessary, reversed.

This transparency makes it easy to review a document's history, resolve discrepancies, and avoid mistakes caused by working from outdated information. Annotation and collaboration tools support structured review processes without losing control over who changed what.

Version control is not just about convenience—it's about knowing exactly what was approved and when. For compliance purposes, audit trails, and legal defensibility, this clarity is essential.

Step 4: Apply Password Protection and Encryption

Password protection and encryption add critical layers of security for documents containing sensitive information. While these terms are sometimes used interchangeably, they serve different but complementary purposes.

Password protection restricts who can open, edit, or print a document. Users must enter the correct password to perform the protected action.

Encryption converts document contents into unreadable data. Without the correct credentials—a password or digital certificate—the file cannot be decrypted and remains inaccessible.

When to Use Password Protection and Encryption

Apply these protections to:

- Documents containing personal, financial, medical, or proprietary information
- Files shared externally with clients, partners, vendors, or contractors
- Records subject to regulatory requirements (HIPAA, GDPR, PCI-DSS, etc.)
- Any document where unauthorized access would cause harm

Best Practices

Use strong passwords: Combine uppercase and lowercase letters, numbers, and symbols. Avoid easily guessed passwords.

Consider certificate-based encryption: For high-sensitivity documents, digital certificates provide stronger protection than passwords alone.

Combine with other controls: Password protection and encryption work best alongside access controls, secure sharing methods, and proper handling procedures.

Foxit PDF Editor provides straightforward options for password protection and encryption that integrate into everyday workflows. Security doesn't have to be complicated—it just has to be consistent.

Step 5: Redact Sensitive Information

Redaction permanently removes content from a document. Unlike simply covering text with a black box or highlighting it in dark colors, proper redaction eliminates the underlying data entirely. Once redacted, the content cannot be recovered, revealed, or extracted—even by examining the file's code.

What Redaction Addresses

Comprehensive redaction should address both visible and hidden content:

- **Visible content:** Text, images, graphics, and any visual element that displays sensitive information.
- **Hidden data:** Metadata (author names, creation dates, revision history), embedded objects, annotations, comments, and layered content that may not be immediately visible but remains in the file.

Common Redaction Use Cases

- **Legal discovery:** Removing privileged, irrelevant, or protected information before producing documents.
- **Public records requests:** Protecting personal information in documents released under FOIA or similar regulations.
- **Financial documents:** Removing account numbers, social security numbers, or other sensitive identifiers before sharing.
- **Healthcare records:** Protecting patient information in compliance with HIPAA when sharing documents for research, audits, or other purposes.

A Critical Warning

Simply placing a black box over text, using highlight tools, or changing text color to match the background is not redaction. The underlying content remains in the file and can be easily revealed by copying and pasting, adjusting display settings, or examining the document's code. Improper "redaction" has led to high-profile data exposures in legal, government, and corporate contexts.

Use proper redaction tools that permanently remove content. Foxit PDF Editor includes built-in redaction capabilities that search for and remove sensitive information—including hidden metadata—with confidence that the data is truly gone.

Step 6: Sign Documents Securely

Electronic signatures have become essential for business operations, enabling documents to be signed in seconds from anywhere, on any device. But not all signing methods are equally secure. A truly secure signature workflow includes authentication, audit trails, and legal compliance.

Electronic Signatures vs. Digital Signatures

Electronic signatures (eSignatures) verify identity and confirm intent when approving documents. Secure eSignature solutions include authentication methods (email verification, access codes, identity verification), audit trails documenting when and where signatures occurred, and support compliance with legal standards like the ESIGN Act, UETA, and eIDAS.

Digital signatures go further by using digital certificates from trusted authorities to validate identity. They apply tamper-evident seals—any modification after signing is detectable. Digital signatures are cryptographically bound to the document and remain valid for years, providing strong legal defensibility.

Benefits of Secure Signing Workflows

Faster approvals: Documents are signed in minutes, not days. No printing, scanning, mailing, or chasing down signers.

Clear accountability: Audit trails document exactly who signed, when, where, and from what device.

Legal defensibility: Properly executed eSignatures and digital signatures are legally binding and hold up in court.

Reduced risk: Secure signing methods prevent forged, disputed, or tampered signatures.

Foxit eSign provides secure signing workflows with authentication, audit trails, and compliance features—enabling fast, legally binding document approvals without sacrificing security.

Step 7: Digitize Paper Documents

Paper documents are inherently difficult to secure. They can be lost, stolen, damaged, or destroyed. They cannot be encrypted, password-protected, or access-controlled. They are difficult to search, track, or audit. And they exist in only one place at a time, creating single points of failure.

Digitizing paper documents brings them into secure, manageable workflows where the full range of security controls can be applied.

Benefits of Digitization

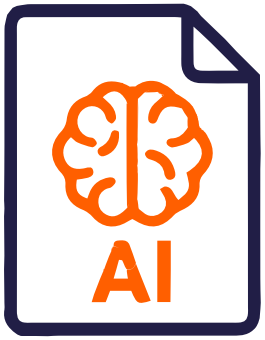
- **Security controls:** Digitized documents can be encrypted, password-protected, and access-controlled like any other digital file.
- **Searchability:** OCR (Optical Character Recognition) converts scanned images into searchable, indexable text.
- **Backup and disaster recovery:** Digital files can be backed up, replicated, and stored off-site. Paper destroyed in a fire or flood is gone forever.
- **Reduced physical storage:** Once digitized and verified, paper originals may be securely destroyed, freeing physical space and reducing the risk of unauthorized access to paper files.
- **Accessibility:** Digital documents can be accessed from anywhere, supporting remote and distributed teams.

Scanning Options

High-volume digitization projects may use office scanners with automatic document feeders. For smaller batches or on-the-go capture, mobile scanning apps convert photos into clean, properly oriented PDFs. Once scanned, documents should be processed with OCR to make the content searchable, then secured with appropriate access controls.

Foxit PDF Editor includes built-in scanning and OCR capabilities, enabling organizations to digitize paper documents and immediately apply security controls—all within a single workflow.

The Role of AI in Secure Document Workflows



Artificial intelligence is increasingly used in document workflows for summarization, translation, data extraction, content generation, and intelligent processing. These capabilities can significantly improve efficiency—but they also introduce security considerations that must be addressed.

Security Risks of External AI Platforms

When documents are processed by external AI platforms, several risks emerge:

Data transmission: Document content is sent to third-party servers, potentially crossing jurisdictional boundaries with different privacy laws.

Data retention: AI providers may store uploaded content for model training, quality improvement, or other purposes not disclosed to users.

Compliance violations: Sending certain document types to external AI services may violate HIPAA, GDPR, contractual confidentiality requirements, or industry-specific regulations.

AI hallucinations: AI-generated content may contain errors, fabricated information, or confidently incorrect statements that end up in business documents.

Purpose-Built AI vs. General-Purpose AI

The distinction between purpose-built document AI and general-purpose AI platforms is critical for security:

General-purpose AI platforms (ChatGPT, Claude, Gemini, etc.) are powerful tools, but they require users to copy content out of documents, paste it into the platform, and then manually reassemble results. This workflow creates data exposure and breaks document formatting.

Purpose-built document AI tools like Foxit AI Assistant operate within the document environment. Data stays within governed workflows rather than being transmitted to external platforms. Document structure and formatting are preserved. And the AI is designed specifically for document tasks—translation, content assistance, intelligent processing—rather than general conversation.

AI can enhance document workflows, but it must be integrated securely. Using external AI platforms as unmanaged workarounds creates data exposure risks that undermine the security controls applied elsewhere in the document lifecycle.

Evaluating Document Security Solutions: What IT Leaders Should Look For

When selecting tools for secure document workflows, several factors distinguish solutions that reduce risk from those that create new vulnerabilities.

Vendor Trust and Track Record

How long has the vendor been in business? Who are their customers? Established vendors with enterprise clients—organizations like Google, Microsoft, Amazon, Dell, and Lenovo—have been vetted for security at a level that newer or unknown providers have not. Look for compliance certifications (SOC 2, ISO 27001, HIPAA, GDPR) that demonstrate commitment to security practices.

Comprehensive Security Features

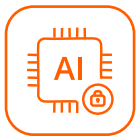
Evaluate the full range of security capabilities: encryption, password protection, permission controls, redaction, digital signatures, and audit trails. A solution that handles only some of these requirements forces you to add other tools—and each additional tool is another potential security gap.

Full Document Lifecycle Support

Can the solution create, edit, convert, combine, secure, sign, and archive documents in a single platform? Reducing handoffs between tools reduces the opportunity for security gaps, data leakage, or workflow friction.

Integration with Existing Systems

Security tools that don't integrate with existing workflows don't get used. Look for solutions that work within Microsoft Office, cloud storage platforms, and the applications employees already rely on. When secure tools are convenient, shadow IT decreases.



AI Integration—Secure and Purpose-Built

If AI capabilities are included, evaluate whether they operate within the document environment or require data to be sent to external platforms. Purpose-built document AI reduces risk while delivering productivity benefits.

Scalability and Administration

Enterprise deployment requires centralized license management, admin controls, policy enforcement, and usage visibility. IT needs the ability to deploy, configure, and govern the solution across the organization—not support dozens of individual installations with no oversight.

The Business Case for Secure Document Workflows

Investing in document security is fundamentally about risk management. The costs of prevention are predictable and manageable; the costs of a breach are unpredictable and potentially catastrophic.

Risk Reduction

- Reduce likelihood of data breaches and associated costs (average $4.35M globally, $9.44M in the US)
- Maintain compliance with regulatory requirements and avoid fines
- Protect customer relationships and brand reputation
- Reduce legal exposure from improperly handled documents

Operational Benefits

- Consistent processes reduce errors and rework
- Faster approvals with secure signing workflows
- Better visibility into document status, access, and handling
- Reduced support burden when tools are standardized and well-integrated

When you control how documents are created, shared, and stored, you control your risk. Security and compliance are at the foundation of effective document management—not optional add-ons to be addressed later.

Conclusion: Taking the Next Step

Secure document workflows are not optional—they are essential for protecting sensitive information, maintaining compliance, and preserving the trust of customers, partners, and employees.

Security must be built into every stage of the document lifecycle: creation, editing, sharing, signing, and archiving. Fragmented tools and ad-hoc practices create gaps that put organizations at risk. The cost of a breach—financial, regulatory, and reputational—far exceeds the cost of implementing proper controls.

Standardizing on a comprehensive, secure document platform from a trusted vendor reduces risk while improving efficiency. Look for solutions that support the full document lifecycle with encryption, permissions, redaction, secure signing, and purpose-built AI—backed by a company with the track record and enterprise relationships to prove its commitment to security.

Control your documents, and you control your risk. The time to strengthen your document security is now.

Learn More

Foxit has been a leader in PDF technology since 2001. Trusted by Google, Microsoft, Amazon, Dell, Lenovo, and organizations worldwide, Foxit provides the document security solutions that enterprises rely on to protect sensitive information and maintain compliance.

Foxit PDF Editor delivers comprehensive document security: create, edit, encrypt, password-protect, redact, and manage PDFs with enterprise-grade controls. Built-in OCR digitizes paper documents. Integration with Microsoft Office and cloud platforms keeps security seamless.

Foxit eSign provides secure electronic signatures with authentication, audit trails, and compliance with global legal standards. Route documents for signature, track progress, and close approvals with confidence.

Foxit AI Assistant brings purpose-built AI into your document workflow—translation, content assistance, and intelligent processing—without the data exposure risks of external AI platforms.

One platform for the entire document lifecycle. Enterprise-grade security. Compliance certifications. A vendor you can trust.

Explore how Foxit helps organizations build secure document workflows. Visit **www.foxit.com** to learn more.

The new standard for AI-powered document productivity

www.foxit.com