DocuWare

Document Archiving

Security and Safety Standards

Security breaches, data loss, version management headaches and litigation against regulatory violations has become so common that it all feels like “normal” business.

But often these problems are entirely self-inflicted. Businesses frequently choose weaker security standards because it’s easier or it sounds too complicated and they don’t know where to begin. These companies may also fail to implement processes that ensure information integrity and transparency because they don’t believe that their company is at risk.

Stronger organizations that take serious measures for document safety rarely fall victim to these mistakes.

Why the security of documents matters

Documents are a core element that keeps your business running. This treasure chest of data should always be protected. Ask yourself these questions and it quickly becomes clear.

For organizations:

- Are we protected against deliberate or accidental security breaches from within?
- Are we protected against external hacking threats?
- Can we recover our information in case of a natural disaster?
- Can we defend ourselves against accusations of data mismanagement?
- Are we protected against heavy financial penalties?

For users:

- Can I access the document I need at the moment I need it?
- Do I have confidence that I am looking at the right version?
- Can I safely store my business information without it being accessed by unauthorized viewers?
- Do I have a process for maintaining retention periods for legally sensitive information?
- Am I trained to prevent social hacking and social engineering attacks?

This document outlines modern security and safety standards for archiving and using documents and provides guidance when searching for a document management software provider.

1

Encryption and access rights

Start at the platform's very foundation. How is digital data secured? What are the weakest points between systems? How can access to information be controlled? How is an organization protected from information breaches cyberattacks and theft?

Encryption and access rights

Authentication

All documents should be accessible only through authenticating a unique username and password. This not only allows specific access rights to be assigned, but ensures a complete audit trail of which document was accessed, by whom, and what actions were taken.

Data Traffic

All traffic between systems and components should be encrypted with HTTPS. Unsecured traffic leaves systems wide open to hacking. HTTP lacks the security layer TLS/SSL and allows hackers to intercept critical data such as passwords and financial data.

Access Control

Access to documents requires multiple levels of control. On one hand, entire groups can have access to a broad category of documents. On the other side, those same groups require access to what they can *do* with a document. Access rights must also be possible at an individual level.

For example, a member of HR can access most employee documents like resumes and performance reviews. Employees and their managers can access performance reviews. And employees can also access their financial and insurance information at an individual level.

Furthermore, it should be possible to restrict access to a document based on that document's index data, the key points of metadata used to describe a document's content and purpose.

Encryption

Documents should be encrypted with a key no less than 256 bits long. AES (256 bits) is military-grade encryption and is the current standard of the US government for classified documents at top secret level that must be prepared for future attacks.

2

Redundancy and virus protection

Data storage redundancy is another pillar of information safety. If one system fails, will the backups ensure continuity for your organization? Redundancy and the protection of data against malware is necessary to maintain absolute peace of mind throughout the organization.

Redundancy and virus protection

Active redundancy

Any document management software, whether in the cloud or on-premises, should have at least two levels of storage redundancy. In addition, a third level of geographically segregated redundancy protects against natural disasters.

These fail-safes are a key advantage of modern cloud systems. By leveraging the cloud infrastructure services of a provider like Microsoft, major data centers across the world can be leveraged to synchronously and seamlessly protect information. Other cloud infrastructure providers include Google, Amazon and Oracle.

Data sovereignty

For many organizations, keeping their information within sovereign borders is extremely important. US companies typically do not want their data stored in South America; companies in the EU do not want their data stored in North America unless they conduct business there. Cloud providers must ensure all data – and all data backups – stay within the borders that legally protects the customer and his or her data.

Protection against viruses and malware

Cryptoviruses embed themselves in documents and deliver their payload when opened on a user's local device. Document management systems must actively protect against these malicious threats so neither the user's environment nor the software platform itself are threatened.

3

Retention and compliance policies

Once encryption, access rights and storage redundancy are established, the organization must determine how information itself is managed. Retention policies dictate what gets saved and when the data may be destroyed. Regulatory compliance provides legal guidance on the handling of information.

Retention and compliance policies

Retention policies

Certain types of documents must be kept within an organization for a legally mandated number of years. For example, invoices must be retained for seven years in the US (but ten years in Germany) before their deletion is allowed.

Previously, this was done with paper-based processes managed within shelves full of boxes, and shredded page by page through a monitored machine. Digital document management solves that – but the rules still apply. And a document management system must provide the workflow tools to enact protection or destruction at predetermined times in order to keep your business protected against litigation.

Key compliance initiatives and regulations

The past few decades have seen renewed interest in securing information, whether protecting the rights of individuals through the management of their data by a third party, fiscal transparency and more.

For example:

- **HIPAA:** The US Health Insurance Portability and Accountability Act protects consumers in the US about the use, disclosure and safekeeping of individually identifiable health data
- **CCPA:** The California Consumer Privacy Act is a set of data transparency, data access and privacy rights for citizens of California, USA
- **GDPR:** The General Data Protection Regulation is a set of European rules and standards designed to protect the personal data or personal identifiable information of individuals through data governance
- **Sarbanes-Oxley:** Prevents accounting errors and fraudulent reporting practices through accurate information disclosures

4

Integrity and auditing

Documents must have complete integrity every time they're accessed. The most rock-solid encryption standards and narrow access rights don't mean much if the authenticity of the document itself cannot be trusted.

Integrity and auditing

Electronic signatures

Users should be able to sign documents with a legally valid electronic signature. A **qualified electronic signature** is the most secure signature level. According to the European regulation on electronic identification and trust services for electronic transactions (eIDAS), the legal validity of a qualified electronic signature corresponds to that of a handwritten one. This kind of e-signature ensures the signature is legitimate and the document has not been manipulated because an authorized Trust Service Provider has issued the digital certificate and authenticated the signer.

Logging of changes

The only way to conduct accurate and thorough audits is to record every access, annotation and workflow state of a particular document. That way, an entire history can be reconstructed. This should be easily accessible as a CSV or other common file format.

Version management

Part of maintaining document integrity is understanding what exactly has changed between document versions and ensuring users are only ever editing the most current version. Locking "checked out" documents keeps changes from occurring and maintains an accurate record of who changed what.

5

Industry standards that matter

There are a number of country-specific and internationally recognized standards for system quality, security and feature completeness. When researching where to house – business-critical documents, ensure your provider meets these crucial standards.

Examples of security standards and official regulations

Overall quality of the software and cloud provider

- **ISO 9001:** Excellent Rating Quality control in the production/manufacturing of software
- **ISO 15489:** Proven, reliable and established concepts and principles for business records management
- **ISO 27001:** Highest requirements for the production, introduction, operation, monitoring, maintenance and improvement of a document management system for information security
- **ISO 27017:** Maximum data security for the cloud; the data is protected against access by third parties and only the customer can access it at any time
- **CSA:** Hosting requirements for security, privacy, compliance and risk management set forth in the Cloud Controls Matrix of the Cloud Security Alliance
- **Keypoint Intelligence / Buyer's Laboratory:** Independent analysis for the industry of specialized office products
- **SOC:** SOC, or Service Organization Controls, are a series of standards that focus on a service organization's controls relevant to security, availability, processing integrity, confidentiality, and/or privacy.

  There are several levels of SOC compliance. For example, SOC 2 Type 1 status proves compliance at a single point in time. The more rigorous Type 2 audit measures ongoing compliance. Service organizations include cloud software (SaaS) providers.
- **NIST SP 800–171:** Standards and guidelines for protecting information systems of US federal agencies

For handling financial documents

- **GoBD (Germany):** Tamper-free, long-term archiving according to the German Commercial Code HGB and Tax Code AO
- **Agencia Tributaria (Spain):** Requirements of the Spanish tax authorities for archiving scanned paper documents
- **GeBüV/AccO (Switzerland):** Ordinance on the Maintenance and Retention of Accounts, Switzerland

6

Safe document archiving vendor checklist

When evaluating document management and document workflow software, start with the security and safety of the candidate system. This foundation must be totally reliable: it supports the information that matters to your business. Without it, other features and capabilities don’t matter.

Safe document archiving vendor checklist

A checklist can help you make a fair evaluation between candidate systems when it comes to measuring security, compliance and safety features.

Does the system ...

- ✓ Authenticate through individual username and password system?
- ✓ Send all data between web-based components through HTTPS?
- ✓ Enable group, role, individual and document-centric access rights?
- ✓ Provide modern 256-bit encryption?
- ✓ Actively backup all data and store it in a geographically separated area?
- ✓ Store data within legally sovereign borders?
- ✓ Protect against malicious cryptoviruses and malware?
- ✓ Enable workflow to enact retention policies?
- ✓ Help you meet specific compliance standards for information handling?
- ✓ Retain the document's' integrity using electronic signatures?
- ✓ Log all changes to create a complete audit trail?
- ✓ Manage active and past versions of documents?
- ✓ Achieve recognized third-party security and quality standards?
- ✓ Enable secure integration with other corporate systems like CRM and ERP?
- ✓ Assure non-repudiation?
- ✓ Ensure maximum uptime and availability?
- ✓ Provide 24/7 support?

DocuWare

About DocuWare

DocuWare is a leading provider of document management and workflow automation solutions. Together with its 800+ strong partner network, DocuWare has helped approximately 17,000 customers across 100+ countries simplify their work through digitizing, automating and transforming key processes.

start.docuware.com