



WHITE PAPER: Security and Data Protection for Online Document Management Software



Overview

This paper explores security elements that you should consider as you investigate cloud-based document management.

As organizations transition documents and company information to Software as a Service (SaaS) applications that are no longer inside their own firewalls, inevitable questions about security and data privacy arise. Every company that trusts a third-party with data storage should understand whether their vendor has the security and data privacy measures in place to protect sensitive information.

Security refers to both physical infrastructure – such as the data center where the documents are stored – and the application features that provide passwords, encryption and secure data transfer. Security features ensure that the system is not compromised, either via direct physical tampering or via malicious external attacks. There are also security features that protect data within the organization by keeping it on a need-to-know basis only.



Data privacy is the concept that the personal and sensitive information pertaining to an individual should be treated in a certain

fashion to prevent its misuse. There are guiding principles as to how personal and sensitive data should be treated, and these principles are codified in the data protection and privacy laws of many countries. For example, the language of the European Commission (EC) Data Protection Directive (95/46/EC) has been incorporated into the laws of European countries.

Physical Security

Some document management vendors use infrastructure provided by Amazon Web Services (AWS) for application hosting and data storage. This gives these providers an advantage because services like Amazon Elastic Compute Cloud (EC2) for application processing and the Amazon Simple Storage Service (S3) for document storage are well proven from a security perspective.

Amazon provides a regularly-updated paper on its security features that is available here: <http://aws.amazon.com/security>

Key highlights of Amazon's security measures include:

1. SAS70 Type II Compliance

In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). SAS70 certifies that a service organization has had an in-depth audit of its controls (including control objectives and control activities), which in the case of AWS relates to operational performance and security to safeguard customer data.



AWS has successfully completed a SAS70 Type II Audit, and has obtained a favorable opinion from its independent auditors. When evaluating document management solutions, it is important to ensure that their infrastructure complies with SAS70 Type II.

2. Data Centers

AWS has many years of experience in designing, constructing, and operating large-scale datacenters which are housed in nondescript, hardened facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

All physical access to datacenters by AWS employees is logged and audited routinely. AWS requires that staff with potential access to customer data undergo an extensive background check (as permitted by law) commensurate with their position and level of access to data. It is a major concern if your document management solution is not leveraging this kind of secure data center.

Application Security

Application security refers to the features and measures that are built into the application to guard against threats, attacks and vulnerabilities. Many involve user name and password requirements, encryption, limitation on sign-in attempts and the use of roles and permissions to restrict access to certain data and documents.





1. Passwords

A frequently used mode for user authentication is via integration with Microsoft Active Directory (AD) via LDAP. This allows those organizations using AD to ensure that established password complexity and reset rules apply. For some document management vendors, it also allows system administrators to manage authentication and authorization for both your document management solution and the rest of their enterprise network in one place.

Even without Active Directory integration, a mature document management solution will have the following measures in place for passwords:

- Require users to possess a unique user ID, company name, and password to ensure that those who access the system are authorized to do so
- Inform users of an error when they fail to enter valid credentials (company name, user name, or password); a generic message prevents an unauthorized user from gaining information from sign-in errors
- Show password characters as dots on the login screen so they can't be viewed by anyone nearby

2. Encryption

Secure document management solutions provide encryption of documents in transit via SSL. The protocol allows applications to communicate across a network in a way designed to prevent eavesdropping and tampering. It also provides endpoint authentication and communications confidentiality over the Internet, so that documents sent from a client workstation to the document management service are secure.



3. Roles and Permissions

Roles, groups and permissions to allow or restrict access to documents are an important attribute for keeping documents in the right

hands. You should be able to create as many roles as you need and assign permissions on a per folder or per document basis. With a combination of carefully crafted roles, access to documents can be limited based on a user's function within the organization or a specific business process. You can also structure access based on geography, division, department or any number of variations.

This flexibility ensures that documents are accessible only to the users who need to see them. Using roles to present users with the most relevant information and tools makes their jobs easier and more streamlined.



4. Backup & Disaster Recovery

Document management solutions that use Amazon have an advantage for disaster recovery. Data stored in Amazon S3 is redundantly stored in multiple physical locations as part of normal operation of those services. Amazon S3 ensures object durability by storing objects multiple times across multiple datacenters on the initial write and then actively doing further replication in the event of device unavailability or detected bit-rot.

Document management databases typically contain metadata and configurations. In the case of Amazon as an infrastructure provider, these elements are stored by your document management solution in EC2 and backed up into S3. Amazon's use of massive redundancy ensures that immediate failover can occur from one server to another, if needed. This means that you don't lose valuable time in the event of a natural disaster or server failure.

Document management solutions should take daily snapshots of your working data every two hours and retain them for the previous 24 hours. They should keep a rolling 7 days' worth of daily snapshots, a rolling weekly snapshot for a minimum of 4 weeks and monthly backups for a year. All backups

should be replicated to a second database server.

Data Protection and Safe Harbor

Concepts of data privacy differ among nations and regions, making it difficult to adopt privacy practices that satisfy all governments and their citizens. The European Union (EU) has developed eight principles for data protection, and each nation within the EU was required to incorporate these principles into their own data protection acts.

For example, the Data Protection Act of 1998 codifies the EU principles into law in the United Kingdom (UK). Although not a member of the EU, the Personal Information Protection and Electronic Documents Act (PIPEDA) brings Canada into compliance with the requirements of the European Commission's directive on data privacy.



The United States sees privacy differently than the EU, and in fact, there is no single or overarching right to privacy in US law. Rather, different types of privacy rights have been established on a case-by-case basis by the US Supreme Court through interpretation of various constitutional amendments. Many individual states also protect privacy and data to varying degrees.

Because of these differences, the US has not incorporated the EU principles into federal law, which initially put the US at a disadvantage when dealing with European nations and citizens.

One particular provision of the EU regulations states that data may not leave the EU unless the receiving or hosting country ensures adequate protection for the data, equivalent to that of the EU. To help US entities ensure this adequate level of protection, the US Department of Commerce, in consultation with the EU, created what is known as the Safe Harbor framework.



Data Protection Principles According to European Commission Directive (95/46/EC)

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions (schedule 2 and 3) is met and the Data Subject has given his or her consent to the processing

- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- Personal data shall be accurate and, where necessary, kept up-to-date
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- Personal data shall be processed in accordance with the rights of Data Subjects under this Act
- Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of Data Subjects in relation to the processing of personal data

Organizations have the ability to self-certify and publicly state that they comply with the Safe Harbor framework. Self-certification must be renewed annually, in writing, with the US Department of Commerce. All organizations that have completed self-certification are listed on a public website at <https://www.export.gov/safeharbor>.

Amazon has already obtained a safe harbor certificate for their infrastructure and services. Because document management solutions often serve global customers and they may contain personal and sensitive information, they must comply with the EU principles via the Safe Harbor provisions.

In addition to self-certification, document management providers should also validate privacy practices through TRUSTe, a leading Internet privacy services provider (www.truste.com). The TRUSTe badge lends extra assurance that a document management provider takes privacy issues seriously and has earned safe harbor status. It also provides users with an unbiased mediator if there is a complaint regarding privacy practices.

A table in this document describes the seven safe harbor principles.

Conclusion

Moving data offsite to a third-party provider is not a trivial decision. Security should be addressed through investigating the key elements discussed in this paper:

- Use of a cloud service provider like Amazon with a commitment to maintaining military-grade security of its facilities
- Integration with Active Directory to enable individual organizations to extend their own password and security structure to their document management implementation
- Use of SSL for encrypted transmission of documents

- Roles and permissions that provide granular access at the file and folder levels
- Regular backups of customer data and the massive redundancy inherent in the cloud
- Adherence to the principles of data protection via the Safe Harbor framework and TRUSTe verification

About KnowledgeTree

KnowledgeTree offers mid-market companies the power of enterprise-class document management in an intuitive, cloud-based solution. We help professionals like you to regain control over complex business processes like contract, billing, and invoice administration, while boosting savings and collaboration.

Our full-featured tools enable your teams to create, co-author, and coordinate even massive numbers of documents. You increase collaboration and control via reporting, rich process governance, and integration into Microsoft Office and Outlook.



We make administration simple through advanced security controls, integration with LDAP and Active Directory servers, single sign-on, powerful APIs, SAS 70-II secure datacenters, and always-current Cloud-delivered technology.

That's why Orbitz, Miramax, Alcatel / Genesys, Fuji Chemical, ShareCare, and many others like you have joined KnowledgeTree and doubled our client base in just 9 months.

KnowledgeTree continuously monitors emerging security issues and will incorporate the latest security methods and protocols into our product as they become available.

For more information, please visit www.KnowledgeTree.com.



Safe Harbor Principle

Notice: Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.

Choice: Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

Onward Transfer (Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Security: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data integrity: Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Enforcement: In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.