DocumentSync Security, Compliance, & Privacy

Foveonics has developed an Electronic Document Management System named DocumentSync. DocumentSync is a cloud-based, full featured EDMS. Users can securely access their document repositories in the cloud and can search and retrieve documents securely from their PC, laptop, or mobile device. DocumentSync is built on Microsoft web technologies and is designed to be a heterogeneous application that can be accessed using popular web browsers such as: Microsoft Edge, Google Chrome, Mozilla Firefox, and Apple Safari. DocumentSync is hosted in Amazon Web Services (AWS) Cloud infrastructure. AWS Cloud provides compliance programs, security policies, data durability, scalability, and redundancy thus ensuring business continuity and disaster recovery preparedness, and 99.9999% guaranteed uptime.

Foveonics provides full business continuity and disaster recovery solutions to our clients. Documents stored within DocumentSync reside in AWS Cloud thus ensuring high availability and business continuity. Foveonics can also provide hot site services for electronic document storage. Additionally, Foveonics can provide several disaster recovery and business continuity copies of scanned documents. After a conversion project is complete Foveonics provides the client with a hard drive of the images and index data. This copy can be used to access files in case cloud-based systems are not available (internet outage, etc.).

Security Practices & Technologies

Password Policies - DocumentSync Cloud supports industry-standard password controls, such as password minimum length, complexity and history.

Vulnerability scanning - Foveonics performs a vulnerability scan of backend servers that run in the DocumentSync Cloud hosting environment.

Penetration testing - Foveonics engages third-party vendors to conduct external penetration testing of the DocumentSync Cloud system.

Intrusion detection - DocumentSync Cloud utilizes host-based intrusion detection systems to reduce the risk of data theft by individuals or organizations attempting to gain unauthorized access.

Firewalls - DocumentSync Cloud's firewall configuration settings are regularly reviewed based on industry standards.

Repository application auditing - DocumentSync Cloud supports auditing of both access and modification of objects in repositories.

Access rights - Administrators can configure access rights and privileges to limit actions that users can perform across the repository based upon role assignments or group memberships.

Fine-grained access control - Administrators can use access rights to limit and control access to individual documents and objects. For example, security tags restrict access to documents on a document-by-document basis.

Repository audit log - The DocumentSync Cloud repository audit log includes details of user actions, including viewing, modifying, creating and deleting documents, and similar operations on metadata and other repository objects.

Architecture Security

Tenant isolation - DocumentSync Cloud provides tenant isolation by logically segregating customer data between accounts. Customers do not have access to any other customer's data or services.

Encryption - DocumentSync uses AES-256 encryption to encrypt customer data. Connections over the Internet to DocumentSync Cloud are encrypted using HTTPS over TLS 1.2 or higher. Requests over unencrypted HTTP will be automatically redirected to the equivalent HTTPS endpoint.

Business Continuity and Disaster Recovery - DocumentSync Cloud is hosted in multiple regions. Regions consist of multiple availability zones that are comprised of multiple data centers. These data centers are housed in separate facilities with redundant power, networking and connectivity.

Compliance Programs

The AWS Compliance Program helps customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance Enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment.

IT standards Foveonics comply with are broken out by Certifications and Attestations; Laws, Regulations and Privacy; and Alignments and Frameworks. Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance.

The following is a list of compliance programs Foveonics currently maintains:

Cloud Security Alliance

CJIS

HIPAA

FISMA

SEC Rule 17a-4(f)

Privacy

At Foveonics, we have embraced a culture of privacy, which includes embedding privacy-by-design in our engineering efforts, and have implemented controls and policies throughout our organization. Foveonis endeavors to continually adapt and adhere to ever-evolving regulations that apply to its business.

Operationally, we strive to keep our stakeholders' data secure and retain only information we collect from you where we have an ongoing legitimate business need to do so, like providing you with a service you have requested, or to comply with applicable legal, tax or accounting requirements.

At Foveonics, all employees are required to complete annual privacy training which covers applicable privacy regulations and best data handling practices.

We collect information that you provide directly to us only for legitimate business purposes. For example, when you manage your user profile, participate in interactive features (such as the Contact Us page), request newsletters or other marketing communications, request customer support, enter login information, or otherwise communicate with us.

You have the right to opt-out of marketing communications we send you at any time. You can exercise this right by clicking on the "unsubscribe" or "opt-out" link in the marketing e-mails we send you.

For personal data transferred from the United Kingdom, the European Union and Switzerland, we will provide appropriate safeguards, such as through use of standard contractual clauses and compliance with EU-U.S. and Swiss-U.S. Privacy Shield requirements. To learn more, visit the "International Transfers" section of the Privacy Notice.