Laserfiche Cloud Security and Compliance

Laserfiche Cloud provides a scalable and secure environment for organizations across industries to automate processes, centralize content and address compliance requirements.

Security

Advanced data protection for your content with Laserfiche Cloud's robust security, administrative controls and advanced audit trail capabilities.

- **Tenant isolation** - Laserfiche 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 in transit** - All data sent between Laserfiche customers and applications is encrypted in transit using Transport Layer Security (TLS) with Perfect Forward Secrecy (PFS).
- **Encryption at rest** - Data-at-rest in Laserfiche Cloud is protected using industry-standard AES-256 encryption.
- **Vulnerability scanning** - Laserfiche performs a vulnerability scan of backend servers that run in the Laserfiche Cloud hosting environment.
- **Penetration testing** - Laserfiche engages third-party vendors to conduct external penetration testing of the Laserfiche Cloud system.
- **Intrusion detection** - Laserfiche Cloud utilizes host-based intrusion detection systems to reduce the risk of data theft by individuals or organizations attempting to gain unauthorized access.
- **Firewalls** - Laserfiche Cloud's firewall configuration settings are regularly reviewed based on industry standards.
- **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.
- **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.
- **Multi-factor authentication** - Multi-factor authentication can be enabled for a Laserfiche Cloud user account.
- **Single sign-on** - Laserfiche Cloud supports single sign-on with Active Directory Federation Services (ADFS) and Security Assertion Markup Language (SAML).

- **Password policies** - Laserfiche Cloud supports industry-standard password controls, such as password minimum length, complexity and history.

- **Repository audit log** - The Laserfiche 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.

- **Repository application auditing** - Laserfiche Cloud supports auditing of both access to, and modification of, objects in repositories.

Compliance

With Laserfiche, governance and compliance can be a seamless part of how your organization operates.

- **SOC 2 Type 2** - This report details the controls for Laserfiche Cloud related to the criteria for the security, availability, and confidentiality principles set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

- **Privacy regulatory compliance** - Laserfiche addresses privacy regulatory requirements in Laserfiche Cloud and as part of our business operations. This includes the California Consumer Privacy Act (CCPA) as well as leading international privacy standards such as the General Data Privacy Regulation (GDPR) of the European Economic Area. For more information, see: https://www.laserfiche.com/legal/privacy/.

- **International data transfers and EU/Swiss/U.S. Privacy Shield Framework compliance** - Laserfiche complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal data transferred from the European Union to the United States. Laserfiche has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. For more information, see: https://www.laserfiche.com/legal/privacy/#privacy-shield-framework-compliance.

- **Data processing agreement** - Laserfiche's Cloud Subscription Agreement incorporates, by reference, a standard data processing agreement for customers with operations in the European Economic Area.

- **WORM Compliance for SEC 17a-4** - Laserfiche Vault is a solution package of services and cloud-based features that supports stringent non-alterable record archival requirements such as WORM (write once, read many) compliance required by SEC Rule 17a-4 for broker dealers. Beyond financial services, Laserfiche Vault's strict compliance mode can also be applied to support rigorous records management practices for electronically stored information (ESI) requiring prevention of any unauthorized alternations or deletions of digital records.

- **Voluntary Product Accessibility Section 508 Compliance** - Laserfiche has published VPATs available for Web Client, Public Portal and Federated Search.

Reliability

Laserfiche's preventative, detective and corrective controls reduce risk while increasing uptime and availability.

- **Business continuity and disaster recovery programs** - Laserfiche Cloud SaaS services are 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.

- **Laserfiche Cloud service levels** - Laserfiche publishes a status page that displays the current status of Laserfiche Cloud applications, maintenance notices and outage reports.

- **Automated backups** - Laserfiche Cloud customer data is backed up multiple times per day. Backups are retained for defined periods with support for point in time recovery. All backup data is encrypted. Backup data is replicated and stored in geographically separate data centers. Backup and restoration is tested on at least a quarterly basis.

Records Management

Easily manage the lifecycle of documents and get notified when documents are ready for disposition.

- **Auto-filing and classification** - Auto-file newly created records according to industry regulations and corporate policies, and automatically classify and apply disposition schedules and other retention policies to incoming records.

- **Notifications** - Automatically notify records managers when a record needs to be archived or destroyed based on the record type.

- **Deployment across devices** - Enforce records management policies across all devices including mobile phones, tablets, laptops and desktops by storing only one copy of a record in a centralized repository.

- **Disposition schedules** - Automatically classify and apply disposition schedules and other retention policies to incoming records.

- **Record transparency** - Provide business units with multiple ways to view records without impacting the overall file plan and allow users who are not records managers to access documents without exposing the records management design.

- **Records management search filters** - Allow records managers to search for records based on retention schedules or cut-off dates.

- **Centralized location for records** - View the record timeline, modify properties of records, record folders, and record series, and perform record actions such as cutoff or final disposition, all from a single location.