everlaw

Security and Compliance at Everlaw

Everlaw prioritizes data security and privacy with enterprise-class security protocols and privacy standards because we understand that hosting sensitive client data on a SaaS ediscovery platform requires an established compliance program and rigorous controls.

Everlaw's security and compliance program is holistic and part of our core philosophy. It demonstrates our commitment to ethics and our company values, as well as compliance with our security, privacy, and confidentiality commitments to customers, and applicable laws and regulations. Our program is built on top of federal guidance on effective compliance programs because we believe that security, privacy, and compliance go hand-in-hand.

For any inquiries about our security and compliance program or to access our SOC 2, ISO 27001, or Cyber Essentials Plus reports, please email us at security@everlaw.com.

Everlaw's ediscovery solutions meet rigorous security, privacy, and compliance standards.

FedRAMP Authorized

SOC 2 Type 2 Certified

Supports HIPAA Compliance

Supports GDPR Compliance

ISO 27001:2013 Certified

Cyber Essentials Plus Certified

Adding value for our customers

Everlaw delivers value to users instantly and scales on-demand thanks to its highly secure, cloud-native architecture built on Amazon Web Services (AWS). Security and compliance are a critical part of our core philosophy, and influence all aspects of our business, from product design and development, marketing, sales, and customer service.

COMPLIANCE PROGRAM FRAMEWORK

The Everlaw Compliance Program Framework has seven elements and is based on the United States Sentencing Commission Guidelines Manual, Section 8: Effective Compliance and Ethics Program, the U.S. Justice Manual, Section 9-28.800 on Corporate Compliance Programs, and the U.S. Department of Justice's Evaluation of Corporate Compliance Programs. Everlaw's program is also based upon the thirty-two Security & Privacy-by-Design Principles developed by the Secure Controls Framework. Everlaw's dedicated Security & Compliance team is accountable for the design, execution, and operation of the company's security, privacy and compliance program based on this framework.

ENTERPRISE RISK MANAGEMENT

Everlaw adopted the Three Lines of Defense governance model for its system of internal control. This model is designed to ensure the effective and transparent management of compliance obligations and risks by making accountabilities clear across the organization. Everlaw's process for risk assessment and management is a key governance and management function for all departments and is based on the NIST Risk Management Guide for Information Technology Systems, NIST SP 800-30. The Security and Compliance team is accountable for scheduling periodic risk assessment meetings with the Risk Management Committee, maintaining and updating the Risk Register, as well as monitoring risk response actions and progress.

POLICIES & PROCEDURES

Everlaw documents and disseminates appropriate policies and procedures that give both content and effect to norms supporting a culture of ethics and compliance. They also serve to address the compliance, security, and privacy risks identified by the company via the risk assessment process described above. Everlaw's Policies and Procedures address information security, business policies and practices, and federal-specific and government-specific compliance requirements.

AVAILABILITY & BUSINESS CONTINUITY

Everlaw's uptime exceeds 99.95% annually, including scheduled maintenance windows. Everlaw has a business continuity and disaster recovery plan that incorporates input from periodic risk assessments, vulnerability scanning and threat analysis, as well as third-party and vendor risk profiles. The business continuity and disaster recovery plans and incident response procedures are tested at least annually and inform the ongoing risk assessment and management process.

"Everlaw makes it easy to track important documents and compile notes from multiple reviewers.

Everlaw's analytics help us understand what progress we've made on our project and how much longer we'll work before we finish. This is good information to have when you're planning out the schedule of a long project."

G2 User Review

Government Administration

DATA PROTECTION & PRIVACY

Everlaw has implemented the appropriate safeguards to protect its customer's data against any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access. Team data inventories and data protection impact assessments are updated and reviewed by the Everlaw Privacy team regularly. Everlaw has a SOC 2 Type 2 certification relevant to the Privacy criteria.

In addition, Everlaw has engaged independent auditors to review its compliance status for both HIPAA and GDPR. The Everlaw Privacy Policy explains how information is collected, used, stored, and disclosed by Everlaw. More information is available at everlaw.com/privacy.

INCIDENT REPORTING & RESPONSE

Everlaw's incident reporting and response procedure aligns with NIST SP 800-61 guidance on handling incidents and contains a clear escalation path, as well as steps for breach notification. All incidents are logged in an incident tracking system that is subject to auditing on an annual basis. Our procedure takes a variety of scenarios into consideration, including insider threats and software vulnerabilities, and it is tested at least annually.

PERSONNEL SECURITY

All employees and select suppliers undergo comprehensive background checks prior to the first day of working at Everlaw, including criminal history and employment verification in accordance with local laws. Everlaw also verifies work eligibility for all employees by collecting I-9 documents and running E-Verify checks. Additionally, all Everlaw employees, upon joining the company and/or during their employment period, as well as certain service providers, are required to sign non-disclosure and confidentiality agreements. Everlaw requires employees to affirm their acknowledgment and agreement to follow Everlaw's Code of Conduct, Employee Handbook, and all Policies and Procedures on an annual basis.

CORPORATE IT SECURITY

Everlaw requires full-disk hard drive encryption for all computers and controls employee access to customer and personal data using role-based access, multi-factor authentication, and account management procedures. Our standards require a 256-bit AES algorithm for full-disk encryption, installation of antivirus software, and strong passwords. Everlaw's information security policy establishes requirements for password complexity, changes, protection, reuse, and follows NIST best practices.

Mobile device access is only allowed on permitted devices that are configured in accordance with the company's bring-your-own-device (BYOD) policy. The mobile device policy allows the removal of Everlaw data from the device if it is lost or stolen. Everlaw has a secure virtual private network (VPN) for remote access to office resources.

The Security and Compliance team monitors employee access requests and changes, enforces the clean desk and BYOD policies, and works with the Everlaw IT team to ensure secure machine configuration for all employees.

TRAINING & AWARENESS

All Everlaw employees complete security, compliance, and data privacy training upon hire and annually thereafter. Additionally, all employees, regardless of their tenure, participate in annual live security and privacy training. Specific role-based training is required upon hire and on an annual basis. The Security and Compliance team conducts security and privacy awareness campaigns and provides updates via email, posters, presentations, and supplemental materials. In addition to security and privacy, our program includes training for all employees on important regulatory and compliance issues such as AML, Antitrust, and Gifts & Entertainment.

THIRD-PARTY RISK MANAGEMENT

Everlaw has an extensive third-party supplier and vendor management program, which requires a security and privacy assessment, led by the Security and Compliance team, to verify that appropriate technical and organizational measures are in place and to meet Everlaw's privacy and security requirements. In addition to the Security and Compliance team, Operations and Finance teams also perform formal reviews of all vendors and suppliers prior to contract execution.

INDEPENDENT ASSESSMENTS & CERTIFICATIONS

Everlaw's system of internal control requires annual independent third-party audits to test the operational effectiveness of our program and practices. Annual audits include SOC 2 Type 2 (Security, Privacy, Confidentiality & Availability), ISO 27001:2013, Cyber Essentials Plus, and FedRAMP hosted on AWS GovCloud. Customers can request a copy of Everlaw's current certification documentation by emailing **security@everlaw.com**. For US government customers, Everlaw's FedRAMP security package can be found on the **FedRAMP Marketplace**.

> "We didn't want to introduce technology and disrupt things and have it not easily adopted. Everlaw helped us do that. It helped us with an ease of adoption."

Chris McDaniel
President and CEO,
Cognicion

ACCESS CONTROLS

Everlaw enforces role-based access controls. Employees are granted a limited set of default permissions to access company resources, such as company email and internal company portals. Privileged access requires formal account management and access control procedure that involves review and approval from a line manager or other executives, as dictated by Everlaw's security policies. All requests are logged and managed to maintain the audit records.

PHYSICAL SECURITY

Everlaw limits access to its corporate offices to identified authorized individuals who require access for the performance of their job function and authorized visitors. All visitors are required to sign in to gain entry, and must be escorted by an employee. Everlaw terminates the physical access of individuals promptly when access is no longer required. Access to Everlaw corporate offices is managed and monitored by the Security and Compliance team.

DATA CENTER SECURITY

Everlaw is hosted in secure AWS cloud servers. We operate in several jurisdictions using AWS cloud hosting infrastructure, for example: US (US East and West Regions), Canada (Central Region), Australia (Asia Pacific, Sydney Region), UK (London Region), and EU (Frankfurt Region). AWS has SOC 1, 2, and 3, ISO 27001, and FIPS certifications, in addition to meeting compliance standards for many other legal, security, and privacy frameworks. Everlaw's Federal Cloud is hosted on AWS Gov Cloud, both have FedRAMP authorization and both are operated by U.S. citizens on U.S. soil. You can read more about AWS' compliance practices and certifications here: Security Practices and Security Compliance.

SECURE ARCHITECTURE

Everlaw's architecture leverages AWS to host the application, all customer data, and backups. The Amazon Virtual Private Cloud (VPC) allows our services to operate in separate, virtual networks that are isolated from other external traffic, except where access is explicitly allowed via firewalls.

As part of our AWS Customer Responsibility, Everlaw implements secure architecture in our AWS-hosted cloud environment. This includes endpoint protection on hosting environments, including antivirus, which are updated with critical patches or security releases in accordance with Everlaw's server change control procedures.

Additionally, Everlaw utilizes private subnets with private IPs and controls all public traffic with AWS security groups. All communications between the clients and Everlaw — as well as all third-party applications — take place over a secure HTTPS connection using transport layer security (TLS) to ensure data in transit is encrypted. We leverage the default encryption-at-rest provided by AWS, which protects the data on disk with AES-256 encryption.

APPLICATION SECURITY

We take steps to securely develop and test against security threats to ensure the safety of our customer data. Everlaw maintains a Secure Development Lifecycle, in which training our developers and performing design and code reviews takes a prime role. Proper error handling and logging, input validation, and encryption are all part of the SDLC.

Everlaw leverages modern and secure open-source frameworks with security controls to limit exposure to OWASP Top 10 security risks. These controls reduce our exposure to SQL Injection (SQLi), Cross Site Scripting (XSS), and Cross Site Request Forgery (CSRF), among others. Everlaw engineers participate annually in secure code training covering OWASP Top 10 security risks, common threat agents, and Everlaw security controls. In addition, on at least an annual basis, Everlaw employs third-party security experts to perform detailed penetration tests on our web application.

SECURITY AND RELIABILITY MONITORING

Everlaw has an on-call team to respond to specific alerts. Through vulnerability scanning, the use of intrusion detection and intrusion prevention systems, and by subscribing to industry and government alerts (e.g., US-CERT), we keep a continuous watch on the security of our customers' data. Everlaw's monitoring program uses a combination of open-source and commercial tools such as Host Intrusion Detection Software (HIDS). We also leverage security logs generated by AWS firewalls to monitor suspicious activity. Everlaw security and site reliability engineers actively monitor alerts on our system configuration and any anomalies.

DATA SECURITY

Everlaw customers' data is encrypted, whether it is in transit or at rest. We use hybrid encryption techniques that constitute software-based encryption, hosting solutions (AWS), and self-encrypting drives to align with NIST Special Publication 800-53.

Encryption In Transit: Everlaw serves application data using HTTPS to ensure encryption in transit of all customer data. The Everlaw application uses Transport Layer Security (TLS) version 1.2 or higher to protect HTTPS communications. For email security, our platform leverages opportunistic TLS encryption (OE) by default.

Encryption At Rest: Everlaw leverages the default encryption-at-rest provided by AWS, which protects the data on disk with AES-256 encryption. We also configure all snapshots to encrypt backup data. Additionally, Everlaw encrypts data at rest using AES-256 to secure inactive data stored on any device or network.

As part of our system of internal control and SDLC, Everlaw implements data protection and privacy by design principles. When developing a new feature or a new product, we implement the appropriate organizational and technical safeguards to ensure that personal data is only processed for a specific purpose. At Everlaw, we follow our strict information security policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of our customer data.

DATA BACKUP & DELETION

Everlaw backs up client data multiple times per day. Everlaw takes advantage of AWS storage classes, which stores data across multiple Availability Zones in the applicable AWS Geographic Region. These physically separated and isolated Availability Zones are connected with low latency, high throughput, and highly redundant networking. Everlaw users with delete permissions in database settings can delete documents from the database. On a customer's request, upon termination or expiry of a contract, Everlaw will return or delete all customer data.

VULNERABILITY MANAGEMENT

Everlaw has an ongoing vulnerability management program that utilizes a variety of vulnerability scanning tools to assess its internal and external network environments against emerging security threats, including OWASP Top 10 security risks. These tools are carefully configured to match our infrastructure requirements and are updated monthly. Everlaw has an established process to log, prioritize, and remediate discovered vulnerabilities. As described above, in addition to our internal scanning and testing program, Everlaw employs an independent testing team to perform vulnerability scanning and penetration testing on at least an annual basis.

PRODUCT SECURITY FEATURES

Everlaw has a variety of product security features. We have highlighted a few below.

Single Sign-On (SSO): Everlaw supports single sign-on (SSO) via the SAML 2.0 protocol, allowing customers to log into Everlaw via their organization's existing LDAP or other SSO system.

Multi-Factor Authentication (MFA): Additionally, Everlaw offers multi-factor authentication (MFA) ***at no additional cost*** for all customer accounts, which can be enforced at the organization level. Multi-factor authentication increases your account's security by requiring a second method for logging in, such as access to your email or mobile device.

Granular Permissions: The ability to specify access to tools, data, and work products is crucial to secure and efficient review. On Everlaw, admins can use fine-grained permission settings to precisely grant users access to what they need to do their jobs well.

Analytics & Monitoring: The Everlaw Analytics page gives you a view of all user activity on your project. From here, you can monitor live and historic activity of all users on your project, as well as all administrative activity.

Secure In-Platform Sharing: Everlaw's in-platform project messaging allows for direct sharing and secure communication between users, enabling users to bypass the typical process of downloading and sharing documents with colleagues via email and other forms of workplace communication.

Flexible Sharing Options: Often, a review requires a third-party expert or co-counsel to access documents in order to complete a review project, offer an expert opinion, or manage project consultants. Everlaw users can organize, create, and share an appropriate subset of documents in a secure project, eliminating the risk of providing complete access to the entire document corpus.

Location Approval Lists (IP Range Blocking): With the increase of remote work, security concerns have become more top-of-mind for legal and IT professionals. Everlaw gives organizations more control over who has access to projects by allowing project admins to restrict access based on a user's IP address and country. This feature helps organizations better protect their data and, as a result, their clients.