Everlaw

REPORT ON

EVERLAW'S

DESCRIPTION OF ITS EVERLAW PLATFORM AND ON THE SUITABILITY OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, CONFIDENTIALITY, AND PRIVACY

SEPTEMBER 1, 2022 to AUGUST 31, 2023

MARCUM
ACCOUNTANTS ▲ ADVISORS

EVERLAW– SOC 3 TABLE OF CONTENTS

Acronym Table

AES	American Encryption Standard
AICPA	American Institute of Certified Public Accountants
API	Application Program Interface
AWS	Amazon Web Services
CEO	Chief Executive Officer
ELK	Elasticsearch
EU	European Union
Everlaw	Everlaw, Inc.
GRC	Governance, Risk and Compliance
HTTPS	Hypertext Transfer Protocol
ISO	International Standards Organization
IT	Information Technology
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OWASP ZAP	Open Web Application Security Project Zed Attack Proxy
SaaS	Software as a Service
S3	Simple Storage Solution
SDLC	Software Development Lifecycle
SOC	System and Organization Controls
SP	Special Publication
SQL	Structured Query Language
TLS	Transport Layer Security
TSP	Trust Service Principles
UK	United Kingdom
URL	Uniform Resource Locator
US	United States
USA	United States of America
VPC	Virtual Private Cloud

Section 1: Assertion of the Management of Everlaw

Assertion of the Management of Everlaw

We are responsible for designing, implementing, operating, and maintaining effective controls within Everlaw's Everlaw Platform (system) throughout the period September 1, 2022 to August 31, 2023, to provide reasonable assurance that Everlaw 's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (*With Revised Points of Focus- 2022*), in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2022 to August 31, 2023, to provide reasonable assurance that Everlaw's service commitments and system requirements were achieved based on the applicable trust services criteria. Everlaw's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period September 1, 2022 to August 31, 2023, to provide reasonable assurance that Everlaw's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Megha Thakkar

Senior Director GRC

Everlaw, Inc.

October 12, 2023

Section 2: Independent Service Auditors' Report

MARCUM
ACCOUNTANTS ▲ ADVISORS

Independent Service Auditors' Report

To: Everlaw

Scope

We have examined Everlaw's accompanying assertion titled "Assertion of Everlaw Management" (assertion) that the controls within Everlaw's Everlaw Platform (system) were effective throughout the period September 1, 2022 to August 31, 2023, to provide reasonable assurance that Everlaw's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus- 2022),* in AICPA *Trust Services Criteria*.

Service Organization's Responsibilities

Everlaw is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Everlaw's service commitments and system requirements were achieved. Everlaw has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Everlaw is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Everlaw's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Everlaw's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Everlaw's Everlaw Platform were effective throughout the period September 1, 2022 to August 31, 2023, to provide reasonable assurance that Everlaw's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Marcum LLP

Tampa, Florida

October 12, 2023

Attachment A: Everlaw's Description of its Everlaw Platform

System Description

Company Overview and Services Provided

Everlaw, based in Oakland, California, with regional offices in New York, Washington, D.C and London, England, develops and manages the Everlaw Platform. Everlaw customers include legal firms, corporations, journalists, non-profit organizations and government entities engaged in litigation, investigations, data subject access requests and other types of large-scale document review and analysis projects or collaboration activities.

The Everlaw Platform is a modern, cloud-based eDiscovery and litigation platform that enables teams to process, manage, review, produce, and present electronically stored information in an efficient, powerful, and cost-effective manner. Storybuilder by Everlaw is a standalone collaborative tool for legal professionals that enables teams to organize documents and build cohesive narratives.

Infrastructure

The Everlaw Platform is a cloud native and web browser-based SaaS technology platform that is accessed via the internet. The web application features file and document uploading via secure protocols, as well as feature-rich search, review, and collaboration functions for preparing a case, investigation or other relevant workflow. The platform APIs enable seamless integration with other technology systems. Everlaw Platform are enabled in the United States, Canada, United Kingdom, Europe (Germany), and Australia.

Amazon Web Services (AWS)

The system components that make up the Everlaw Platform are hosted within AWS data center facilities, specifically US (US East and West Regions), Canada (Central Region), Australia (Asia Pacific, Sydney Region), UK (London Region), and EU (Frankfurt Region). A separate partition of the Everlaw Platform is hosted within AWS GovCloud (US). Each of these AWS regions hosts an independent installation of the Everlaw Platform in an isolated VPC. Each VPC is a multi-tenant environment that users access via a VPC-specific URL (app.everlaw.com, app.everlaw.ca, etc.). Everlaw relies on AWS to provide appropriate physical and logical protections and processes for the AWS data center facilities.

The Everlaw Platform components allow for the management and configuration of a project database and active projects that use the project database. The Everlaw Platform uses relational databases (MySQL and PostgreSQL) and AWS S3 buckets for storage.

Storage

Private AWS S3 buckets store customer files that represent project case documents or user task output; they are organized by project case database.

Management Subnet

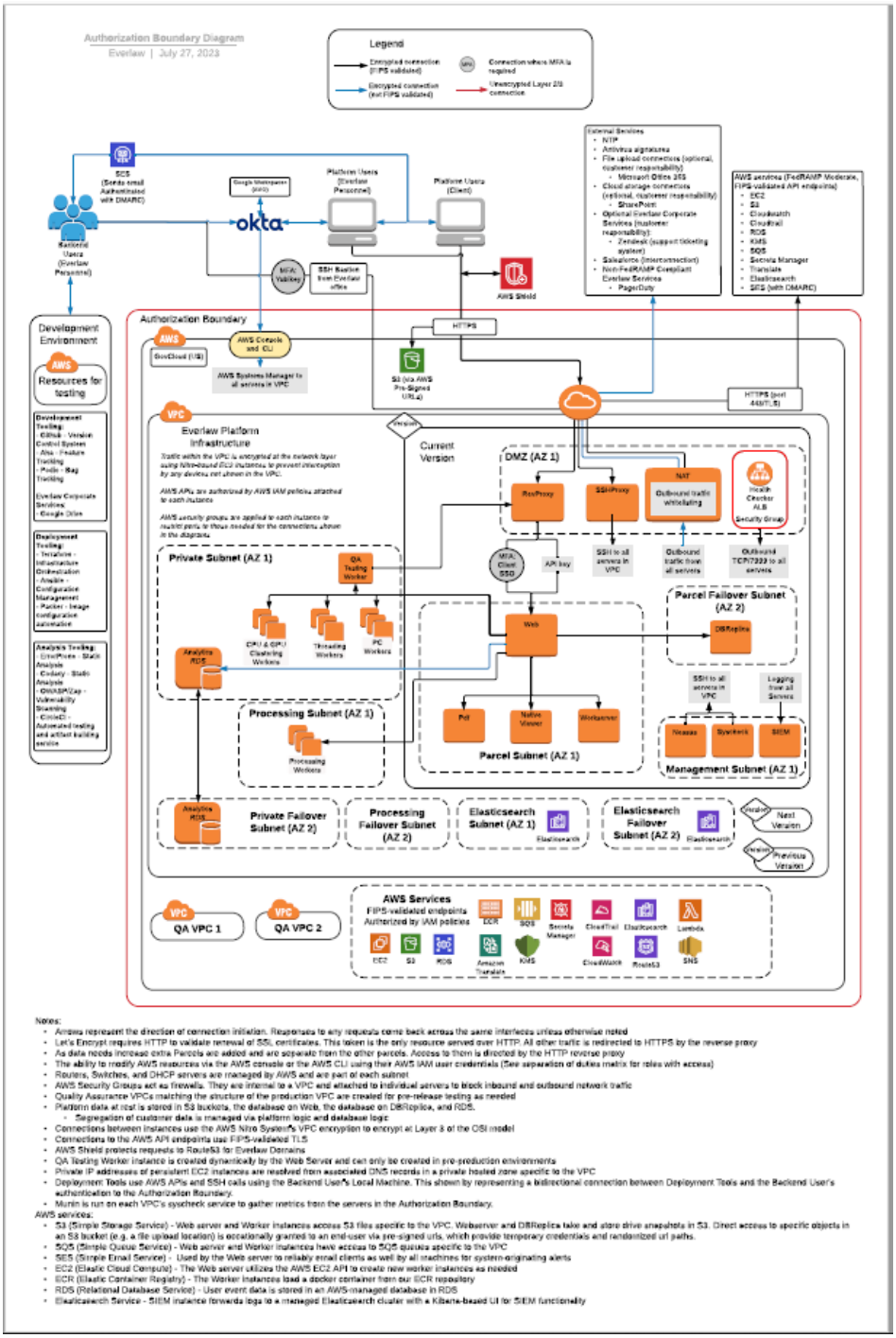
Each VPC contains a management subnet that provides the Everlaw environment with security and management functionality. This includes logging and monitoring, vulnerability scanning, and other management tools. Access to this environment is strictly restricted to Everlaw personnel only, over encrypted channels using MFA.

System Diagram/Boundaries

The system boundary includes a dedicated system interconnection with AWS that provides the underlying hardware and operational environment that powers the Everlaw Platform. Thus, the Everlaw Platform relies on AWS for the purposes of storing, processing, and transmitting customer data. Everlaw retains complete control and ownership of the customer data. The Everlaw Platform includes features that rely on external services. The external services include (previously described):

- Google Cloud Translate API
- Zendesk

System Diagram



Notes:

- Arrows represent the direction of connection initiation. Responses to any requests come back across the same interfaces unless otherwise noted
- Let's Encrypt requires HTTP to validate renewal of SSL certificates. This token is the only resource served over HTTP. All other traffic is redirected to HTTPS by the reverse proxy
- As data needs increase extra Parcels are added and are separate from the other parcels. Access to them is directed by the HTTP reverse proxy
- The ability to modify AWS resources via the AWS console or the AWS CLI using their AWS IAM user credentials (See separation of duties matrix for roles with access)
- Routers, Switches, and DHCP servers are managed by AWS and are part of each subnet
- AWS Security Groups act as firewalls. They are internal to a VPC and attached to individual servers to block inbound and outbound network traffic
- Quality Assurance VPCs matching the structure of the production VPC are created for pre-release testing as needed
- Platform data at rest is stored in S3 buckets, the database on Web, the database on DBReplica, and RDS.
  - Segregation of customer data is managed via platform logic and database logic
- Connections between instances use the AWS Nitro System's VPC encryption to encrypt at Layer 3 of the OSI model
- Connections to the AWS API endpoints use FIPS-validated TLS
- AWS Shield protects requests to Route53 for Everlaw Domains
- QA Testing Worker instance is created dynamically by the Web Server and can only be created in pre-production environments
- Private IP addresses of persistent EC2 instances are resolved from associated DNS records in a private hosted zone specific to the VPC
- Deployment Tools use AWS APIs and SSH calls using the Backend User's Local Machine. This shown by representing a bidirectional connection between Deployment Tools and the Backend User's authentication to the Authorization Boundary.
- Munin is run on each VPC's sysCheck service to gather metrics from the servers in the Authorization Boundary.

AWS services:

- S3 (Simple Storage Service) - Web server and Worker instances access S3 files specific to the VPC. Webserver and DBReplica take and store drive snapshots in S3. Direct access to specific objects in an S3 bucket (e.g. a file upload location) is occasionally granted to an end-user via pre-signed urls, which provide temporary credentials and randomized url paths.
- SQS (Simple Queue Service) - Web server and Worker instances have access to SQS queues specific to the VPC
- SES (Simple Email Service) - Used by the Web server to reliably email clients as well by all machines for system-originating alerts
- EC2 (Elastic Cloud Compute) - The Web server utilizes the AWS EC2 API to create new worker instances as needed
- ECR (Elastic Container Registry) - The Worker instances load a docker container from our ECR repository
- RDS (Relational Database Service) - User event data is stored in an AWS-managed database in RDS
- Elasticsearch Service - SIEM instance forwards logs to a managed Elasticsearch cluster with a Kibana-based UI for SIEM functionality

Locations and Infrastructure

Everlaw has the following key functions and locations which support the Everlaw Platform:

Function	Location
Business Operations, IT, and GRC	Oakland, California (Headquarters) London (UK) Remote personnel (USA)
Engineering (including Software Development)	Oakland, California (Headquarters) Remote personnel (USA)
Security Engineering	Oakland, California (Headquarters) Remote personnel (USA)
Privacy and Legal	Oakland, California (Headquarters) Washington, DC

Software

The following provides a non-exhaustive summary of services used to deliver (and support delivery of) the Everlaw Platform.

Component	Description
Operating Systems	Operating Systems used to support the Everlaw Platform are Linux
Data Stores	Customer data resides in AWS S3 bucket, SQL, MySQL and Search Index databases
Threat Management	Endpoint protection antivirus Continuous monitoring Incident Response Intrusion detection system
Security Event Logging	VPC-based logging of events (ELK) Centralized log management
Vulnerability Testing and Vulnerability Management	Vulnerability scans of major system components is performed by following tools: OWASP ZAP Nessus
Customer Support	Zendesk is used for customer service management and communications.

Component	Description
Code Repository	GitHub is used as a code repository for the application.
Incident Reporting and Management	Podio is used as an incident tracking and project management system. Bugsnag is used to notify personnel on a server error or when a user encounters a browser error using the website. Pingdom and Site24x7 are used to notify personnel of website downtime.
Customer Records Management and Billing	Salesforce is used for customer account creation, customer records management and billing.
Corporate Environment	Corporate Identity Management System: Okta is used for corporate identity and access management. Email and Document Management: Google Workspace is used for Company email and internal document management systems.

People

Everlaw's CEO is responsible for leading the organization and managing the strategic operations of Everlaw. The CEO is committed to offering a secure product to Everlaw customers.

The following teams are in-scope for this report as their job responsibilities require that they have access to production systems, develop code to be included into the environment or support operational and advisory functions:

Team	Responsibilities Covered
Business Operations	Responsible for managing Facilities, PMO, and Corporate IT teams.
People Operations	Responsible for recruitment, employee engagement, performance management, benefits administrations, HR operations, and LED.
Engineering	Responsible for overseeing the development of new code, fixing bugs, release management process, and maintaining the engineering infrastructure that supports the Everlaw Platform.
Security Engineering	Responsible for creating and operating a secure platform that meets the security and compliance requirements and commitments. Security Engineering manages (not including) Application Security, Security Operations, and Security Incident Response functions.

Team	Responsibilities Covered
Legal	Responsible for and leads the Everlaw legal organization, which ensures that the company grows and scales in a way that takes into account all of the obligations and risks that face enterprises. The Legal organization includes Commercial, Corporate, Product, Corporate Compliance, Legal Operations, Privacy, and the GRC teams.
GRC	GRC is responsible for creating, maintaining, and continuously improving the security, risk, security awareness and training, and compliance programs. The GRC team also includes the Customer Trust function.
Product	Responsible for managing the product development lifecycle, including prioritization and feature definition, and the oversight of the design of the Everlaw Platform.
Customer Success	Responsible for managing Customer Success, Support and Data Operations, Training, User Research, and Customer Success Operations and Enablement functions.

Security Policy, Procedures and Governance Structure

Everlaw has an Information Security Policy in place along with relevant procedures that documents the information security program and required processes. Everlaw has documented relevant procedures to meet the Trust Services Principles. In addition, Everlaw performs a risk assessment to identify risks to the business and systems. Once relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objectives of the organization. Relevant policies and procedures are updated to reflect changes in the design of the controls or addition of any new controls.

Data

As part of using the Everlaw Platform, users may create or upload documents, images, files, annotations, notes, tags or other electronic records relating to litigation or project matters. In the course of providing the service, Everlaw may also collect statistical data and performance information, analytics, meta-data or similar information, generated through instrumentation and logging systems, regarding the operation of the Everlaw Platform, including data about use of the service.

Data processing is initiated by direct ingestion into the Everlaw Platform, receipt of digital files, or by physical media in limited circumstances where a client chooses to send media to Everlaw. Data is processed within the Everlaw Platform, or at the relevant Everlaw office and uploaded to the Everlaw Platform, when necessary. Usage data and analytics can be exported directly by users or Everlaw personnel via the Everlaw Platform.

Control Activities

General Information Systems Controls

Everlaw maintains a formal ISMS that conforms to the requirements of the ISO 27001 standard, including security policies, standards, and procedures. The Information Security Policy and supporting standards have been developed to segregate duties and enforce responsibilities based on job functionality.

Hiring, Onboarding & Staff Development

The Everlaw Human Resources team is responsible for hiring, onboarding and staff development activities. They activities include (but not limited to):

- Background investigations
- Employee offer acceptance
- Employment disciplinary action
- Security awareness and training
- Employee performance reviews

Personal career growth and reward of meeting expectations are driven by periodic performance feedback and demonstrate Everlaw's commitment to advance qualified personnel to higher levels of responsibility. Everlaw employees are required to read and acknowledge the company's internal policies and confidentiality requirements, sign an Everlaw confidentiality agreement, protect the confidentiality of customer managed information, and complete all required training.

Access Management

Everlaw leverages role-based security to limit and control access within the production network. Production access is controlled using least privilege principles. All access to the production environments is logged. Access to the AWS console and the Everlaw Platform administrative pages is via multi factor authentication. Platform access (including production access) is based on a user's role. All access requests are reviewed by the user's manager (minimum requirement) and by other appropriate parties when necessary (e.g. Legal). The ability to create or modify user access accounts and user access privileges in the production environment is limited to system administrators. All requests are logged and managed to maintain the audit records and reviewed on a quarterly basis.

Data Encryption

Everlaw customer data is encrypted, whether it is in transit or at rest. Everlaw uses 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 Platform uses TLS version 1.2 or higher to protect HTTPS communications. For email security, the 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.

In addition, customer passwords are hashed and encrypted at rest within the production database. Encryption keys are protected and restricted within an approved key-management system to appropriate personnel.

Vulnerability Management

The Engineering team performs internal and external vulnerability scans on a periodic basis and tracks identified issues to remediation in accordance with Everlaw's relevant policies. The Security Engineering team and the GRC team meet on a regular basis to discuss security risks, critical vulnerabilities and remediation plans.

Secure Software Development

Everlaw maintains a Secure Development Lifecycle, in which training the developers and performing design and code reviews take a prime role. Proper error handling and logging, input validation, and encryption are all part of the SDLC. Everlaw does not use production data in the development and testing environments during the software development life cycle.

Everlaw leverages modern and secure open-source frameworks with security controls to limit exposure to OWASP Top 10 security risks. These controls reduce exposure to SQL Injection , Cross Site Scripting, and Cross Site Request Forgery, 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 its web application.

Incident Management

Everlaw's incident reporting and response procedure aligns with NIST SP 800-61 guidance on handling incidents and contains a clear escalation path to the senior leadership and the CEO, as well as steps for breach notification. All incidents are logged in an incident tracking system that is

subject to annual auditing. The procedure takes a variety of scenarios into consideration, including insider threats and software vulnerabilities, and it is tested at least annually.

All security incidents and site outages must be handled with the involvement and cooperation of the SMT, or others who have been authorized by the SMT. Based on the initial assessment, the SMT will determine next steps according to the Incident Reporting and Response Procedure in order to mitigate risks and prevent future occurrences. Containment is prioritized to ensure the incident does not overwhelm resources or increase damage. The precise containment strategy will vary depending on the specifics of the incident.

Change Management

Changes to both infrastructure and software are developed and tested in a separate development or test environment before implementation. The Everlaw Configuration Management Policy dictates that all changes must be documented and approved by the Configuration Change Review Group. In addition, any changes that may have an effect on the security of the Platform undergo Security Impact Analyses to assess what mitigating actions are required. All changes are tested and approved prior to its release into the production environment. Emergency changes follow the formalized change management process, wherein reviews and approvals are documented prior to deployment, but at an accelerated pace. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Approvals for network device or configuration changes go through the same change management procedure as application development. Changes must be logged, reviewed for security implications, and approved prior to implementation.

Change management policies and procedures are documented and reviewed annually. Changes are managed through a formal review process. Policies and procedures are provided to Everlaw employees in a shared folder as well as on the company intranet.

Availability

Within AWS, the system is built with geographically dispersed infrastructure and application redundancy across data centers to help ensure service operations resiliency. Database replication between locations occurs in real time, with failover support.

Data Backups

Customer data recorded on Everlaw's Everlaw Platform are backed up according to management's backup policy. Procedures are in place to help ensure that backed up data is secure, available and verified for the integrity of data to help ensure recovery in the event of a failure to primary production systems.

Customer data transmitted through Everlaw's Platform is secured and protected using various access control mechanisms. Everlaw's Platform offers customizable services and reports to meet the specialized needs of clients.

Vendor Management

Everlaw has a formal vendor onboarding program in place. Relevant and applicable vendors are reviewed by the privacy and GRC team. An annual review of critical vendors is performed by the GRC team.

Communication

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. Everlaw's management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed.

Risk Assessment

Everlaw management performs an annual risk assessment, which requires management to identify risks in its areas of responsibility and to implement appropriate measures to address those risks. Everlaw's management reevaluates the risk assessment annually to both update the previous results and to identify new areas of concern. The risk assessment process consists of the following phases:

- Identifying – The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- Assessing – The assessment phase considers the potential impact(s) of identified risks to the business and its likelihood of occurrence.
- Mitigating – The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect identified and assessed risks.
- Reporting – The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and applicable regulations.
- Monitoring – The monitoring phase includes Everlaw management performing monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed.

Attachment B – Everlaw's Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Everlaw designs its processes and procedures related to its Everlaw Platform and Storybuilder by Everlaw (hereafter both together referred to as Everlaw Platform) to meet its service objectives. Those objectives are based on the service commitments that Everlaw makes to user entities, the laws and regulations that govern cloud service providers, and the financial, operational, security, availability, confidentiality, privacy, regulatory and compliance requirements that Everlaw has established for the services.

Security commitments to user entities are documented in the appropriate agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the Everlaw Platform that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect data at rest and in transit.

Availability commitments to user entities are documented in appropriate agreements. Availability commitments are standardized and include, but are not limited to, the following:

- Managing capacity demand through the monitoring and evaluation of current processing capacity and usage rates.
- Meeting Company objectives through authorization, design, development, and monitoring of data backup processes and recovery infrastructure.

Confidentiality commitments to user entities are documented in appropriate agreements. Confidentiality commitments are standardized and include, but are not limited to, the following:

- Information is defined and classified into categories with associated periods.
- Data retention and disposal policies and procedures are documented and in place.

Privacy commitments to user entities are documented in appropriate agreements and in the privacy policy publicly posted on Everlaw's website. Privacy commitments are standardized and include, but are not limited to, the following:

- Personal data is stored, maintained, and utilized in accordance with the publicly posted privacy policy.
- Data disclosures to third parties are permissible only to authorized third parties specified and named in agreements and in the publicly posted privacy policy.
- Inquiries for access, deletion, and retention are fulfilled in accordance with the publicly posted privacy policy in a timely manner.

MARCUMGROUP

Marcum Group is a family of organizations providing a comprehensive range of professional services including accounting and advisory, technology solutions, wealth management, and executive and professional recruiting.

These organizations include:

- Marcum LLP
  www.marcumllp.com
- Marcum Bernstein & Pinchuk
  www.marcumbp.com
- Marcum Insurance Services
  www.marcumis.com
- Marcum RBK Ireland
  www.marcumrbk.com
- Marcum Search
  www.marcumsearch.com
- Marcum Strategic Marketing
  marketing.marcumllp.com
- Marcum Technology
  www.marcumtechnology.com
- Marcum Wealth
  www.marcumwealth.com

MARCUM
ACCOUNTANTS ▲ ADVISORS

Ben Osbrach, CISSP, CISA, QSA, CICP, National Risk Advisory Leader
813.397.4860 ● ben.osbrach@marcumllp.com

Mark Agulnik, CPA, CISA, CIS LI, JD, Regional Advisory Partner-in-Charge
954.320.8013 ● mark.agulnik@marcumllp.com