

# FLUID ATTACKS INC. - APPLICATION SECURITY SOLUTIONS

## THROUGHOUT THE PERIOD JULY 1, 2024, TO JUNE 30, 2025

**To the Management of Fluid Attacks Inc. (herein Fluid Attacks)**

## Scope

We have examined Fluid Attacks' accompanying assertion titled "Assertion of the Management of Fluid Attacks Inc." (assertion) that the controls within Fluid Attacks Application Security Solutions were effective throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (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 Organizations.

## Fluid Attacks Responsibilities

Fluid Attacks 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 Fluid Attacks' service commitments and system requirements were achieved. Fluid Attacks has provided the accompanying assertion titled Fluid Attacks' Assertion (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. When preparing its assertion, Fluid Attacks is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

## Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether 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 American Institute of Certified Public Accountants. 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.

Our examination included:

- 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 Fluid Attacks' 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 Fluid Attacks' service commitments and system requirements based 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 the effectiveness of 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 were achieved based on the

KOMPLEYE

Office Address
1900 Reston Metro Plaza, Suite 600
Reston VA 20190

Telephone: (703)-814-0119
E-mail: info@kompleye.com
Website: www.kompleye.com

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 Fluid Attacks Application Security Solutions were effective throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Fluid Attacks' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Kompleye

**Patricio Garcia, CPA, CISA, CMMC LEAD CCA, CDPSE,**
**ISO 9001 LA, ISO 27001 LA, ISO 9001 LA, HITRUST CCSFP, CITP.**
**Partner**
**Kompleye**
**Reston, VA**
**November 20, 2025**

# FLUID ATTACKS' ASSERTION

Zoho Sign Document ID: 2D30419E-OL0YIAOKKKEI3LCZT2CWDYDHWU06N8H9E-HPT8GVMZ0

**Assertion of the Management of Fluid Attacks Inc. (herein Fluid Attacks)**

We have prepared the accompanying description of Fluid Attacks (service organization) description of its Application Security Solutions titled "Description of the Fluid Attacks Application Security Solutions" throughout the period July 1, 2024 to June 30, 2025 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (With Revised Implementation Guidance – 2022), AICPA, *Description Criteria*, (description criteria). The description is intended to provide report users with information about the "Fluid Attacks Description of its Application Security Solutions" that may be useful when assessing the risks arising from interactions with Fluid Attacks' Application Security Solutions, particularly information about system controls that Fluid Attacks has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Implementation Guidance – 2022), in AICPA, *Trust Services Criteria*.

We are responsible for designing, implementing, operating, and maintaining effective controls within Fluid Attacks Application Security Solutions throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Fluid Attacks' service commitments and system requirements relevant to security were achieved. 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 July 1, 2024 to June 30, 2025, to provide reasonable assurance that Fluid Attacks' service commitments and system requirements were achieved based on the trust services criteria relevant to security (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. Fluid Attacks' 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 July 1, 2024 to June 30, 2025, to provide reasonable assurance that Fluid Attacks' service commitments and system requirements were achieved based on the applicable trust services criteria.

Claudia S. Muñoz

**Name: Claudia Sofia Muñoz**
**Role: Legal Representative**
**Fluid Attacks Inc.**

# ATTACHMENT A

## COMPANY OVERVIEW

Fluid Attacks Inc. ("Fluid Attacks") is a private company established in April 2017 that provides application security solutions. Fluid Attacks is a commercial company based in Clayton, North Carolina and has an office in Colombia under the name Fluid Attacks SAS.

## DESCRIPTION OF FLUID ATTACKS' SERVICES PROVIDED

Fluid Attacks Continuous Hacking is a solution that combines application security testing tools, artificial intelligence (AI), and a hacking team to accurately find and help remediate security vulnerabilities throughout the software development lifecycle (SDLC) and ensure secure deployments.

Fluid Attacks reports risk exposure promptly to its clients and supports them to achieve high remediation rates and guarantee high-quality and secure products to their end users.

Fluid Attacks security testing involves different automated and manual techniques, namely, static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA), cloud security posture management (CSPM), secure code review, manual penetration testing, and reverse engineering. Further, Fluid Attacks uses its own AI tool to sort files in a code repository by their probability of containing security vulnerabilities, thus informing Fluid Attacks hacking team of which files to prioritize in their manual tests to start finding vulnerabilities faster.

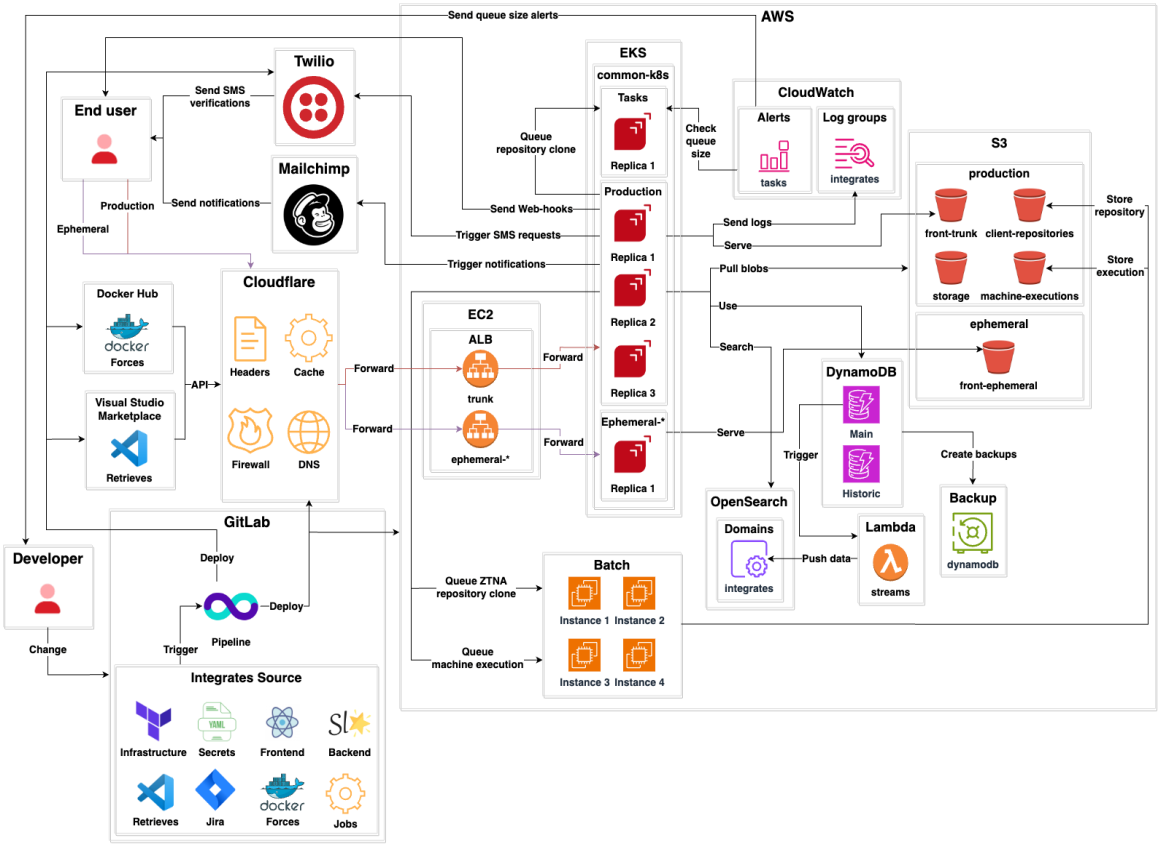
Fluid Attacks helps its clients develop secure software and have secure deployments into production. To ensure secure development, Fluid Attacks performs tests during the entire SDLC. It reports all findings both by its tool and hacking team to its clients on Fluid Attacks platform. There, its clients can learn about the specific lines of code affected, find links to documentation with examples of compliant code, control the remediation process, request retests to verify fixes and keep track of their progress in risk mitigation, among other vulnerability management tasks. To help developers easily incorporate vulnerability management into their workflow, Fluid Attacks offers integrations with several tools developers often use.

Fluid Attacks support in the vulnerability remediation process is through custom and automated fixes generated by AI from Fluid Attacks IDE extension. Additionally, Fluid Attacks feature called "Talk to a Pentester", allows its clients to meet with Fluid Attacks hacking team for guidance on remediation. Further, Fluid Attacks offers a CI agent to prevent the client's development team from deploying software versions with unmanaged vulnerabilities, thus helping to enforce its client's policies and urge the development team to fix the software security issues.

## COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

### INFRASTRUCTURE

Fluid Attacks maintains a system inventory that includes virtual machines (EC2 instances) and computers (laptops). The inventory documents device name, device type, vendor function, OS, location, and notes. To outline the topology of its system, the organization maintains the following architecture diagram:




The Fluid Attacks application infrastructure is located at the EE.UU. East Region (Northern Virginia) and UE Region (Ireland) data centers. Amazon Web Services (AWS) acts as a hosting subservice organization for the company. The subservice organization provides the physical security and environmental protection controls, as well as managed services for Fluid Attacks' infrastructure.

AWS's network security uses software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules.

In addition to the firewall, Fluid Attacks exerts endpoint security through Mobile Device Management (MDM), which includes antivirus and antimalware, and forbids end-users from disabling or altering software.

Fluid Attacks' Information Security and Endpoint Security Policies ensure that all computer devices involved in the Fluid Attacks environment have proper virus and malware protection, current virus definition libraries, and the most recent operating system and security patches installed. The IT department verifies that all known and reasonable defenses are in place. In the event of a virus threat, the specific MDM function will remove or quarantine the infected file.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. Fluid Attacks performs continuous security testing to its own technology to detect potential vulnerabilities to the production environment and corporate data. Email is scanned at the gateway and in the hosted email environment. All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on Fluid Attacks-owned computers, as enforced through the MDM. Fluid Attacks maintains several replacement computers that can replace

workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible.

## SOFTWARE

Fluid Attacks maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation. Critical software in use includes the following: Amazon DynamoDB, Amazon S3, Amazon Simple Queue Service (SQS), AWS Batch, AWS CloudWatch, AWS Elastic Compute Cloud (EC2), AWS Elastic Kubernetes Service (EKS), AWS Identity and Access Management (IAM), AWS Key Management Service (KMS), Cloudflare, Datadog, GitLab, Nix, Okta, Google Workspace, Time Doctor 2, dbt Labs, among others.

## DATA

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements or within the Fluid Attacks Knowledge Base website. Customer data is captured which is utilized by Fluid Attacks in delivering its application security solution.

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. All employees and contractors of Fluid Attacks are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are, subject to limited exceptions, confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to Fluid Attacks' business and finances are, as a matter of Fluid Attacks policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, applications and systems is shared by the IT department. Fluid Attacks engineers are responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under their control, moreover, every Fluid Attacks personnel is required to sign a non-disclosure agreement (NDA).

Fluid Attacks has policies and procedures in place to ensure prior retention and disposal of confidential and private data. The retention and data destruction policies define the retention periods and proper destruction procedures for the disposal of data. These policies are reviewed at least annually. The destruction of data is a multi-step process. Client accounts and data are deleted upon termination of the contract.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Cloud networks are protected by enterprise-class firewalls and appropriate enterprise-class virus protection is in place. Passwords protection with assigned user rights is required for access to the applications and databases. Access to the cloud’s network, applications, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

Data is categorized in the following major types of data used by Fluid Attacks:

| Category | Description | Examples |
|---|---|---|
| **Public** | Public information is not confidential and can be made public without any implications for Fluid Attacks. | - Press releases<br>- Public website<br>- Marketing Materials<br>- Product descriptions<br>- Release notes<br>- External facing policies |
| **Internal** | Non-confidential information or data assets that are not intended for public disclosure can be shared internally within the company without prior approval.<br>Access to internal information is approved by management and is protected from external access. | - Internal policies and procedures<br>- Employee directories<br>- Training materials<br>- Meeting minutes and internal presentations<br>- Publicly available industry research and news<br>- Design documents<br>- Non-sensitive project updates and status reports<br>- Product specifications<br>- Correspondences |
| **Restricted** | Information collected and used by Fluid Attacks to operate the business. Fluid Attacks must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.<br>Access is restricted to employees with a “need-to-know" based on business requirements. This data can only be distributed outside the company with approval. | - Legal documents<br>- Contractual agreements<br>- Employee PII<br>- Employee salaries<br>- Internal reports<br>- Email and chat messages |
| **Confidential** | Information received from customers for processing or storage by Fluid Attacks. Fluid Attacks must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.<br>Highly sensitive data requiring the highest level of protection has restricted access limited to specific employees or departments. The disclosure of such records to others requires explicit approval from a company executive. | - Customer operating data<br>- Customer PII<br>- Customers' customers'<br>- PII<br>- Anything subject to a confidentiality agreement with a customer |

## PROCESSES

Formal IT policies and procedures are in place that describe logical access, computer operations, change management, incident management, and data communication standards to obtain the stated objectives for system and data security, data privacy, and integrity for both the company and its clients and define how services should be delivered. These are communicated to employees and located within the organization's intranet.

Reviews and changes to these policies and procedures are performed annually and are approved by senior management.

**Physical Security and Environmental Controls**

Fluid Attacks' production servers are maintained at the third-party colocation data center, and the physical security and environmental protections are the responsibility of the subservice organization. Management obtains and reviews SOC reports annually to monitor that the protection controls are in place.

**Logical Access**

Fluid Attacks uses an IAM platform for managing access to applications across the company. Logical access to Fluid Attacks' applications and data is limited to properly authorized individuals. Further, Fluid Attacks' infrastructure components always grant minimum privileges only to the applications and personnel that need to use them. Distributed firewall is behind the Fluid Attacks domain that implements full DDoS protection, browser integrity check, hotlink protection, rate limiting, browser integrity check, and anti-bot capabilities. Appropriate firewall rules, managed by top cybersecurity experts, are in place to restrict access to customer data and to limit the possibility of disruptions to customer operations from unauthorized users.

**Computer operations - backups**

Customer data is backed up and monitored by the Engineering Team for completion and exceptions. If there is an exception, Engineering Team will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

**Computer operations - availability**

Fluid Attacks maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

Fluid Attacks internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Fluid Attacks utilizes its own vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

**Change Management**

Fluid Attacks runs an Application Build Process for every change any one developer wants to introduce to Fluid Attacks' source code in the continuous integration and continuous delivery (CI/CD) system via a merge request. Developers also need to ask a peer to review their code changes before their merge requests

can go into production. Peer-reviewers usually evaluate code quality, commit message coherence, and other semantic properties of the change.

CI/CD helps to maintain source code versions and migrate source code through the development process to the production environment. The CI/CD maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Fluid Attacks has a Change Management Policy in place to define requirements for establishing and maintaining baseline protection standards for the company's applications and infrastructure, and to ensure that a standard set of minimum requirements are established for changes that are made to production systems and supporting infrastructure across the organization. The Fluid Attacks Change Management Policy applies to all individuals performing software development tasks and system administration within the organization, as well as to production systems and supporting infrastructure across the organization.

**Patch Management**

Fluid Attacks takes a proactive approach to patch management. Fluid Attacks' entire technology stack is subject to comprehensive, automated, continuous security testing. Further, development projects run continuous integration pipelines, including strict linters and software composition analysis, to ensure that no known vulnerabilities are released to production. The required patches are applied promptly by developers at the Engineering department. The patching process is tracked through GitLab issues.

**Backup and Recovery**

Fluid Attacks maintains backups stored in decentralized data centers. Such backups exist seamlessly for as long as desired, giving Fluid Attacks full traceability and recoverability. Fluid Attacks' databases have daily, weekly, quarterly, and annual full backup schedules. The retention period for these jobs is one week, twelve weeks, three years, and fifteen years, respectively. The database of Fluid Attacks' platform has point-in-time recovery with the ability to recover the database to the state it was in at a specific date and time (hours, minutes and seconds) over the last 35 days.

All backups are encrypted and stored on AWS storage systems.

**Incident Management**

Fluid Attacks maintains an Incident Response Policy that describes the process for identifying and addressing potential security incidents. The policy details exactly what must occur if an incident is suspected and covers incidents such as malfunctions, performance degradation, service disruptions, or errors in Fluid Attacks products or components. Plans for detecting, responding to, and recovering from incidents are included in the policy, and post-incident activity requirements are defined. To ensure responsible employees are prepared to respond to incidents, the organization has communicated and published the process through its Knowledge Base website. Additionally, periodic virtual training is provided to help employees to identify possible security issues.

The organization provides a help channel email where clients can report potential security breaches. Internal users are directed to report incidents through the same channel. For transparency, and to keep stakeholders informed, details about each incident are displayed at https://status.fluidattacks.tech/history.

**System Monitoring**

The Vulnerability Management Policy describes the organization's policies and procedures related to logging and monitoring as well as vulnerability identification and remediation. Fluid Attacks uses Amazon CloudWatch for system logging within the AWS environment. For management purposes on AWS accounts, Fluid Attacks registers events related to them using CloudTrail. The company uses VPC Flow

Logs to capture ingoing and outgoing IP traffic information from network interfaces in the company's VPC. Further, Fluid Attacks uses other tools that give full observability of its source code. The company also uses applications for error tracking, issue management, error monitoring, tracking and alerting.

Amazon GuardDuty is used for threat detection purposes in cloud infrastructure. The tool continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts, Amazon Elastic

Compute Cloud (EC2) workloads, container applications, and data stored in Amazon Simple Storage Service (S3).

Datadog is also used as a visibility and monitoring tool. This is a cloud-based monitoring and analytics platform that provides comprehensive visibility into Fluid Attacks' entire technology infrastructure.

The platform specializes in infrastructure monitoring by tracking server, database, and network performance across cloud services like AWS delivering real-time metrics and automated alerting capabilities. For application performance monitoring, Datadog analyzes application response times, error rates, and provides code-level performance insights while tracking user experience metrics. The platform also serves as a centralized log management system, collecting and analyzing logs from across all systems while enabling powerful search and filtering capabilities that correlate logs with metrics and traces.

The vulnerability assessment process involves the execution of Fluid Attacks' own multi-method tool and Amazon GuardDuty's Malware Protection feature. Moreover, endpoint security through MDM in devices of Fluid Attacks' personnel includes antivirus and prohibits end-users from disabling or altering the software. Alerts are sent immediately when a potential threat is detected, and logs are generated and retained for at least one year with at least three months readily available. Fluid Attacks' scanner keeps up with advisories published on different sources (e.g., GitHub, GitLab, OSSF) to be able to identify newly emerging vulnerabilities and patches required.

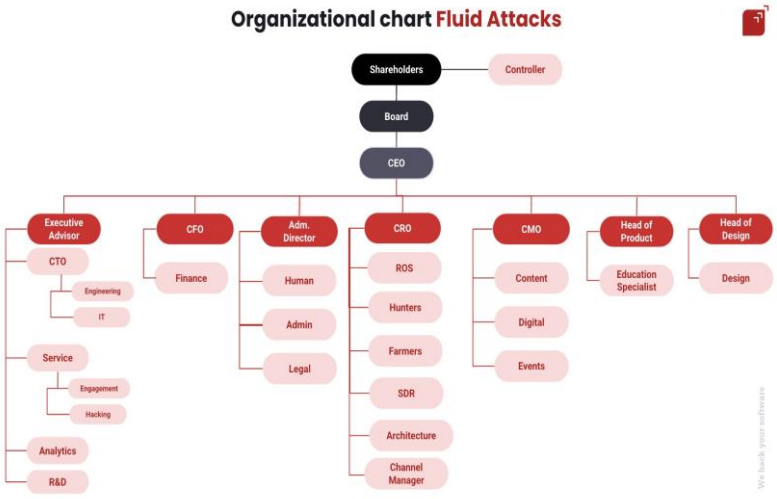
**Third-Party Management**

The organization maintains a Third-Party Management Policy that includes requirements for interacting with service providers. The policy includes requirements for performing due diligence measures prior to engaging with a new provider. Due diligence procedures include requiring of providers an attestation report evidencing SOC 2 and/or ISO 27001 compliance. In cases when the vendor does not supply one of these reports, Fluid Attacks assesses whether the vendor handles data in compliance with applicable data protection laws as well as what other relevant security practices the vendor follows and what certifications it has.

## PEOPLE

The Fluid Attacks staff provides support to the above services. Fluid Attacks employs dedicated team members to handle all major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and recovery. The company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep Fluid Attacks and its data secure.

Fluid Attacks' corporate structure includes the following roles:




- Board - Provides strategic oversight, guidance, and accountability, ensuring that Fluid Attacks operates in the best interest of its shareholders and stakeholders. The Board's responsibility includes oversight of Fluid Attacks' cyber risk management.
- Chief Executive Officer (CEO) - Handles the strategic direction of Fluid Attacks. The CEO assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments.
- Executive Advisor - Responsible for the technological direction and advancements of the organization. Directs the product, engineering, analytics and service teams to efficiently create/present new services, maintain existing ones, and help support the Fluid Attacks customer base using the service.
    - Chief Technology Officer (CTO) - This role is responsible for the development of Fluid Attacks' platform as well as for enhancing and augmenting the capabilities of Fluid Attacks' vulnerability scanner. They are also responsible for daily IT support aspects, including support to end-users with day-to-day issues.
    - Service - This area is responsible for the activities of Fluid Attacks' hacking team and managing client relationships to ultimately achieve the client's objectives in alignment with Fluid Attacks' mission.
    - Analytics - This area is responsible for all of Fluid Attacks analytics, providing the information for the company to make decisions supported on reliable data. Moreover, they are responsible for the ideation of the charts and metrics that are presented to end-users on Fluid Attacks' platform.
    - R&D - This area is responsible for Fluid Attacks' research of vulnerabilities in open-source software projects.
- Chief Financial Officer - Responsible for overseeing all financial activities and strategies to ensure Fluid Attacks' financial health and stability. Their role involves managing financial planning, budgeting, and forecasting.
- Administrative Director - Responsible for administrative support, legal aspects and human resources procedures.
- Chief Revenue Officer (CRO) - Primary role for outbound reach to prospects and completing sales. They are also responsible for the maintenance and renewals of existing customer contracts.

- Chief Marketing Officer (CMO) - Responsible for the outward communication of company initiatives. Primary role responsible for exposing new programs to prospects and existing customers and furthering the public reach of Fluid Attacks.
- Head of Product - This role is responsible for the strategic vision and roadmap of Fluid Attacks' software products, guaranteeing compliance with quality, and therefore security, standards.
- Head of Design - Responsible for developing an intuitive user experience for the Fluid Attacks platform as well as visually appealing designs for Fluid Attacks' products' user interfaces and branding.

# ATTACHMENT B

## SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS (DC2)

Fluid Attacks designs the processes and procedures of its application security system to meet its objectives. These objectives are based on the service commitments made to user entities, the applicable laws and regulations governing the provision of services, and the financial, operational, and compliance requirements established by Fluid Attacks.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online and in the Fluid Attacks privacy policy and terms of use.

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Uptime availability of production systems
- Secrets rotation
- Defined service recovery objectives
- Cloud infrastructure served from multiple zones
- Established backup policies
- Use of device formatting and data removal
- Use of a non-disclosure agreement (NDA) for personnel

Fluid Attacks establishes operational requirements that support the achievement of security relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies and/or procedures around how the service is designed and developed, how the system is operated, how the internal business systems and infrastructure are managed, and how employees are hired and trained. In addition, how to carry out specific manual and automated processes required in the operation and development of the System.