



SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON
MANAGEMENT'S ASSERTION RELATED TO ITS

Goodfire AI Inc's Platform

Relevant to Security

For the period December 15, 2025 to March 15, 2026

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:



Table of Contents

1. Independent Service Auditors' Report.....	1
Scope	1
Service Organization's Responsibilities.....	1
Service Auditors' Responsibilities.....	1
Inherent Limitations	2
Opinion	2
2. Assertion of Goodfire Management.....	3
3. Description of Goodfire AI Inc's Platform.....	4
Company Background	4
Services Provided.....	4
Principal Service Commitments and System Requirements.....	4
Components of the System	5

1. Independent Service Auditors' Report

To the Management of Goodfire AI, Inc. (Goodfire)

Scope

We have examined Goodfire's accompanying assertion titled "Assertion of Goodfire Management" (assertion) that the controls within Goodfire AI Inc's Platform (system) were effective throughout the period December 15, 2025, to March 15, 2026, to provide reasonable assurance that Goodfire's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 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

Goodfire 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 Goodfire's service commitments and system requirements were achieved. Goodfire has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Goodfire 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 Auditors' 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 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.

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 Goodfire'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 Goodfire'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.

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

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 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 Goodfire AI Inc's Platform were effective throughout the period December 15, 2025, to March 15, 2026, to provide reasonable assurance that Goodfire's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



San Jose, California
April 28, 2026

2. Assertion of Goodfire Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Goodfire AI, Inc. (Goodfire) Platform (system) throughout the period December 15, 2025, to March 15, 2026, to provide reasonable assurance that Goodfire's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Goodfire AI Inc's Platform," (description) 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 December 15, 2025, to March 15, 2026, to provide reasonable assurance that Goodfire's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA, *Trust Services Criteria*.

Goodfire'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 the accompanying system description.

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 December 15, 2025, to March 15, 2026, to provide reasonable assurance that Goodfire's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Goodfire AI, Inc. Management

April 2026

3. Description of Goodfire AI Inc's Platform

Company Background

Goodfire is an AI startup focused on fundamental research in the field of mechanistic interpretability. Goodfire is headquartered in San Francisco and was incorporated in December 2023.

Services Provided

Goodfire works with large enterprise customers on research collaborations. Ember is Goodfire's collection of mechanistic-interpretability tools delivered primarily as SDKs and libraries that are deployed and executed within customer-controlled environments. Goodfire also maintains internal research and development tooling used to build, test, and support Ember releases and to conduct internal research.

Ember assists enterprises in understanding and interpreting their proprietary AI models. It is composed of separate research modules with a variety of types of research tooling and can be accessed within a customer's environment. There are often forward deployed engineers or forward deployed researchers assisting customers with implementation, and the Ember platform is continuously updated and enhanced.

As of the date of this report, Goodfire AI, Inc. does not operate a public-facing production application or hosted SaaS platform. The Ember system consists primarily of internally operated research tooling and software distributed to customers in the form of SDKs and libraries, which are deployed within customer-controlled environments. Within scope, Goodfire operates internal development and research environments (e.g., source control, CI/CD and build systems, internal cloud resources, and collaboration/business systems) used to develop and support Ember SDKs and libraries.

Principal Service Commitments and System Requirements

Goodfire AI, Inc. designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Goodfire AI, Inc. makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Goodfire AI, Inc. has established for the services. The system services are subject to the Security commitments established internally for its services.

Goodfire's commitments are set up in annual contracts with customers, or through short pilot programs also under contract. Our system and service commitments are displayed in these agreements. Availability controls are designed to support internal research operations and customer support activities rather than externally committed service-level guarantees.

Security commitments

Currently implemented controls. Goodfire AI, Inc. maintains security controls designed to protect Goodfire-controlled systems used to develop and support Ember SDKs, libraries, and internal research tooling. Security controls include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized access based on least privilege
- Security monitoring and alerting for Goodfire-controlled cloud resources (e.g., AWS-native threat detection capabilities such as GuardDuty) to detect potentially malicious or unauthorized activity
- Vulnerability management processes for internally developed source code and third-party dependencies, including automated dependency vulnerability alerting and update workflows (e.g., GitHub Dependabot), with issues triaged, prioritized, and tracked through remediation to closure
- Operational procedures for managing and responding to information security incidents, including escalation and notification procedures
- Encryption technologies used to protect information in transit and, where applicable, at rest within Goodfire-controlled systems
- Data retention and secure disposal practices for information maintained within Goodfire-controlled systems
- Availability practices designed to support internal research operations and business support activities

Planned future-state controls (if hosted customer-facing services are introduced). If Goodfire AI, Inc. deploys customer-facing services within Goodfire-controlled cloud infrastructure, the organization intends to implement periodic vulnerability scanning and penetration testing of externally exposed components based on risk and contractual requirements. Customer-facing availability commitments, if any, would be defined contractually if hosted services are introduced.

Components of the System

Infrastructure

As of the date of this report, Goodfire does not maintain a client-facing software-as-a-service platform for customers but instead maintains cloud infrastructure for internal research and development. This infrastructure does not store customer production data. Business systems (e.g., CRMs) store business contact information associated with sales and business development.

The infrastructure described below reflects internally managed research environments and development tooling, not customer-facing production services.

Hardware	Type	Purpose (optional)
AWS Elastic Compute Cloud (EC2)	AWS	Compute

Hardware	Type	Purpose (optional)
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage for internal research artifacts, build artifacts, logs, and operational data (excluding customer production data)

Software

Goodfire AI, Inc. is responsible for managing the development and operation of the Ember system including infrastructure components such as servers, databases, and storage systems. The in-scope Goodfire AI, Inc. infrastructure and software components are shown in the table provided below:

System / Application	Purpose
GuardDuty	Security monitoring service used to detect potential threats, malicious activity, and unauthorized behavior within AWS cloud environments.
Adobe Acrobat	PDF management application used to create, review, edit, and electronically sign documents
Amazon Web Services	Cloud infrastructure provider used for internal research; development environments and supporting services
Checkr Dashboard	Third-party service used to conduct and manage background checks for employees and contractors
Docker	Containerization platform used to standardize application deployment and isolate runtime environments
GitHub	Source code hosting and version control system used to manage application source code and software development workflows
Google Cloud SDK	Command-line tools used by engineering personnel to manage and interact with Google Cloud resources
Google Drive	Cloud file storage and collaboration platform used for internal documentation and controlled data sharing
Google Workspace	Enterprise productivity suite used for corporate email, calendaring, document creation, and collaboration
HubSpot	Customer relationship management system used to manage sales, marketing, and customer communications
LinkedIn	Platform used for recruiting activities and professional networking
Microsoft	Enterprise software provider used for productivity tools and business operations
Netlify	Hosting platform used to deploy static product demos (wireframes and static front-end assets). These demos are non-production and are not intended to process or store customer production data.
Notion	Internal knowledge management and documentation platform used for policies, procedures, and operational documentation

System / Application	Purpose
OpenAI	Third-party AI service provider used to access and integrate large language model capabilities
Pave	Compensation management platform used to support employee compensation planning and benchmarking
Postman	API development and testing tool used to validate and document application programming interfaces
Slack	Internal communication platform used for real-time messaging and operational coordination
Vanta	Compliance management platform used to support SOC 2 and other security compliance programs
Zendesk	Customer support platform used to manage and respond to customer support requests
Zoom	Video conferencing platform used for internal and external meetings

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering 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 the company and its data secure.

Goodfire AI, Inc. has a staff of 40+ employees, organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

Operations: Responsible for maintaining the availability and security of Goodfire-controlled internal cloud environments and supporting infrastructure. Access to internal cloud environments is restricted to authorized personnel based on job responsibilities, with elevated access limited to designated operations personnel.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Data

Data as defined by Goodfire AI, Inc., constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the



Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Goodfire AI, Inc.

Category	Description	Examples
Public	Information intended for public release; disclosure would not adversely impact Goodfire AI, Inc.	Press releases; public website content; published research posts
Internal	Non-public operational information used internally; access is restricted to authorized personnel based on job responsibilities.	Internal memos; design documents; product specifications; internal project correspondence
Prospect / Business Contact Data	Business contact and corporate information collected for sales, partnerships, recruiting, and customer communications; may include personal data such as business contact details.	Prospective customer or partner names; work email addresses; company affiliation; communications and meeting notes stored in CRM/sales tools
Company Confidential	Sensitive internal business information that could adversely impact Goodfire AI, Inc. if disclosed; access is restricted to authorized personnel.	Employee PII; compensation data; financial information; contracts; legal documents; vendor agreements; internal security documentation
Customer-Provided Materials (Limited)	Information voluntarily provided by customers during support or collaboration activities that may be subject to confidentiality obligations; as of the report date, Goodfire does not store or process customer production data within Goodfire-controlled systems.	Approved excerpts or sample outputs shared for troubleshooting; emails or documents provided for collaboration/support; customer-provided requirements or configuration guidance (excluding customer-hosted databases and customer production data)

As of the date of this report, the Ember system is not deployed as a hosted service and does not capture, process, or store customer production data within Goodfire-controlled systems. Goodfire AI, Inc. does collect limited business contact information related to sales and partnership activities (e.g., prospective customer names, work contact details, company information, and correspondence) in CRM and sales pipeline tools. This business information is managed in accordance with applicable privacy requirements and any relevant contractual terms.

Customer-controlled environments where Ember SDKs execute, including customer databases and production data, are outside the scope of this report.



All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Goodfire AI, Inc. has policies and procedures in place to ensure proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

Processes, Policies and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Policies and procedures are reviewed at least annually and updated as needed. Changes are authorized by management, the executive team, and control owners, as appropriate.

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

Goodfire AI, Inc.'s internal environment servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Goodfire AI, Inc. reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Logical Access

Goodfire AI, Inc. provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on a quarterly basis to ensure least privilege access.

Operations are responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Goodfire AI, Inc.'s policies, completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, Operations is responsible for deprovisioning access to all in scope systems promptly.

Computer Operations – Backups

Internal operational data and research artifacts stored in Goodfire-controlled systems are backed up and monitored by the CTO and Operations team for completion and exceptions. If there is an exception, CTO and Operations team will perform troubleshooting to identify the root cause and either rerun the backup or remediate it 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

Goodfire AI, Inc. 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.

Goodfire AI, Inc. internally monitors its cloud infrastructure to ensure reliability.

Goodfire AI, Inc. maintains vulnerability management processes for source code and dependencies. For open-source dependencies, Goodfire uses automated dependency vulnerability alerting and update workflows (e.g., GitHub Dependabot) to identify vulnerable dependencies and propose remediation updates. Reported issues are triaged, prioritized based on severity and impact, and tracked through remediation to closure in accordance with internal response expectations.

Change Control

Goodfire AI, Inc. maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing changes to internally developed SDKs, libraries, research tooling, and supporting infrastructure. Change control procedures include change request initiation, documentation requirements, development practices, testing expectations (as applicable), and required approvals.

A ticketing system is used to document change requests and track changes through implementation. Supporting evidence (e.g., peer review, test results, and validation notes, as applicable) is maintained with the associated ticket. Development and testing activities are performed in logically separated environments from internal operational environments. Management approval is required prior to release of SDKs/libraries or deployment of changes to Goodfire-controlled internal environments, and such approvals are documented within the ticketing system.

Version control software is used to manage source code versions and support the release process for SDKs, libraries, and internal tooling. Version control maintains a history of code changes, provides traceability to individual contributors, and supports rollback capabilities when needed.

Data Communications

Goodfire AI, Inc. uses AWS-based infrastructure to support internal research and development environments. Network access to Goodfire-controlled systems is restricted through logical access controls and network configuration (e.g., VPC configuration, security groups, and authenticated access methods). Data transmitted between systems is protected using encryption in transit where applicable (e.g., TLS for HTTPS connections).

As of the date of this report, Goodfire AI, Inc. does not operate a public-facing hosted application that processes customer production data within Goodfire-controlled infrastructure. If customer-facing services are introduced in the future, Goodfire AI, Inc. intends to implement additional monitoring and security testing for externally exposed components, including vulnerability scanning and penetration testing, based on risk and contractual requirements. Goodfire AI, Inc. also conducts periodic reviews of its security program and implements process improvements and cybersecurity enhancements as needed.

Boundaries of the System

The boundaries of the Ember system include the Goodfire AI, Inc.–controlled infrastructure, software, people, procedures, and data used to develop, maintain, distribute, and support Ember SDKs, libraries, and internal research tooling. Systems and processes that do not directly support these activities are excluded from the system boundary.

The Ember system does not include customer data stores or other stateful services operated by Goodfire AI, Inc. Ember SDKs and libraries are deployed and executed within customer-controlled environments, and customers retain responsibility for configuring the SDKs and operating any supporting infrastructure, including databases and other persistence layers. Accordingly, customer-managed databases and related controls (e.g., backup, recovery, configuration management, and access management) are outside the scope of this report.

This report also excludes the underlying cloud hosting services and physical data center operations provided by AWS.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Goodfire AI, Inc.'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Goodfire AI, Inc.'s ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Goodfire AI, Inc.'s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.



Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

The Goodfire AI, Inc. management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Goodfire AI, Inc. can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Goodfire AI, Inc. to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

Goodfire AI, Inc.'s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Goodfire AI, Inc.'s assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Goodfire AI, Inc.'s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Goodfire AI, Inc.'s human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

Goodfire AI, Inc.'s risk assessment process identifies and manages risks that could potentially affect Goodfire AI, Inc.'s ability to provide reliable and secure services to our customers. As part of this process, Goodfire AI, Inc. maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Goodfire AI, Inc. product development process so they can be dealt with predictably and iteratively.

Integration with risk assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Goodfire AI, Inc.'s system; as well as the nature of the components of the system result in risks that the criteria will not be met. Goodfire AI, Inc. addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Goodfire AI, Inc.'s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.



Information and Communications Systems

Information and communication are an integral component of Goodfire AI, Inc.'s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Goodfire AI, Inc. uses several information and communication channels internally to share information with management, employees, contractors, and customers. Goodfire AI, Inc. uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Goodfire AI, Inc. uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Goodfire AI, Inc.'s management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going monitoring

Goodfire AI, Inc.'s management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Goodfire AI, Inc.'s operations help to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Goodfire AI, Inc.'s personnel.

Reporting deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to the Goodfire AI Inc's Platform.

Subservice Organizations

Goodfire AI, Inc.'s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Goodfire's services to be solely achieved by Goodfire's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Goodfire.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met.

Security Category	
Criteria	Controls expected to be in place
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	

Security Category	
Criteria	Controls expected to be in place
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.



Goodfire management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Goodfire performs monitoring of the subservice organization controls, including the following procedures

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

Complementary User Entity Controls

Goodfire's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the trust services criteria related to Goodfire's services to be solely achieved by Goodfire's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Goodfire's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the trust services criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Goodfire.
2. User entities are responsible for notifying Goodfire of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Goodfire services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Goodfire services.
6. User entities are responsible for providing Goodfire with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Goodfire of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.