# MARA STUDIOS PRIVATE LIMITED

## SOC 3 REPORT

FOR

Locus – A Cloud-Hosted
Software Application

INDEPENDENT SERVICE AUDITOR'S REPORT ON
CONTROLS RELEVANT TO SECURITY, CONFIDENTIALITY & AVALIBILITY

October 01, 2024 – February 09, 2025

Attestation and Compliance Services

CertPro

# TABLE OF CONTENTS

# SECTION 1

## INDEPENDENT SERVICE AUDITOR'S REPORT

# INDEPENDENT SERVICE AUDITOR'S REPORT

To Board of Directors
**Mara Studios Private Limited**

**Scope**

We have examined the accompanying "Description of Locus, a cloud-hosted software application" provided by Mara Studios Private Limited throughout the period October 01, 2024 to February 09, 2025 and the suitability of the design and operating effectiveness of controls to meet Mara Studios Private Limited's service commitments and system requirements based on the criteria for Security, Confidentiality, Availability, Processing Integrity & Privacy principles set forth in TSP Section 100 Principles and Criteria, Trust Services Principles and Criteria for Security, Confidentiality and Availability (applicable trust services criteria) throughout the period October 01, 2024 to February 09, 2025.

The description of boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Mara Studios Private Limited, to achieve Mara Studios Private Limited's service commitments and system requirements based on the applicable trust service criteria. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

**Service Organization's Responsibilities**

Mara Studios Private Limited 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 Mara Studios Private Limited's service commitments and system requirements were achieved. Mara Studios Private Limited has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Mara Studios Private Limited 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 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 systems 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:

a. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
b. Assessing the risks that controls were not effective to achieve Mara Studios Private Limited's service commitments and system requirements based on the applicable trust services criteria.

c. Performing procedures to obtain evidence about whether controls within the system were effective to achieve Mara Studios Private Limited'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.

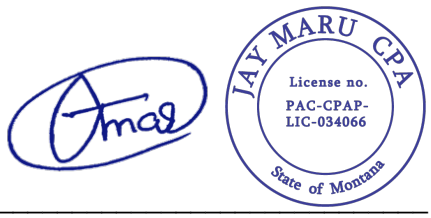
**Inherent Limitations**

There are inherent limitations in 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 Mara Studios Private Limited'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 Mara Studios Private Limited were effective throughout the period October 01, 2024 to February 09, 2025, to provide reasonable assurance that Mara Studios Private Limited's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.




**JAY MARU**
Certified Public Accountant
License Number: PAC-CPAP-LIC-034066
July 04, 2025

# SECTION 2

## MANAGEMENT'S ASSERTION

# MANAGEMENT'S ASSERTION

**Mara Studios Private Limited's Management Assertion for the period October 01, 2024 to February 09, 2025**

We are responsible for designing, implementing, operating, and maintaining effective controls within "Locus, a cloud-hosted software application" throughout the period October 01, 2024 to February 09, 2025, to provide reasonable assurance that Mara Studios Private Limited's service commitments and system requirements relevant to Security, Confidentiality and Availability were achieved. Our description of the boundaries of the system is presented below 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 October 01, 2024 to February 09, 2025, to provide reasonable assurance that Mara Studios Private Limited's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Availability (applicable trust services criteria) set forth in TSP section 100, Trust Services Criteria for Security, Confidentiality, Availability, Processing Integrity, and Privacy (AICPA, Trust Services Criteria). Mara Studios Private Limited's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 October 01, 2024 to February 09, 2025, to provide reasonable assurance that Mara Studios Private Limited's service commitments and systems requirements were achieved based on the applicable trust services criteria.

**For Mara Studios Private Limited**

Signed by:

7B41D6B7F3D0478...

**Authorized Signatory**

# Section 3

## Description of the system

# DESCRIPTION OF THE SYSTEM

**Types of Services Provided**

Locus is a cloud-hosted software application built by Mara Studios Private Limited hereby referred to as Mara.

Locus is Locus's modular, API-first solution enables order-to-delivery excellence by simplifying decision-making for lower costs, greater efficiency, and superior customer experiences across enterprise retail logistics operations.

Any other services provided by Mara Studios Private Limited are not in the scope of this report.

## Principal Service Commitments and System Requirements

Mara Studios Private Limited designs its processes and procedures to meet objectives for its software application. Those objectives are based on the service commitments that Mara Studios Private Limited makes to customers and the compliance requirements that Mara Studios Private Limited has established for their services.

Security commitments to user entities are documented and communicated in Mara Studios Private Limited's customer agreements, as well as in the description of the service offering provided online. Mara Studios Private Limited's security commitments are standardized and based on some common principles.

These principles include but are not limited to, the following:

- The fundamental design of Mara Studios Private Limited's software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
- Mara Studios Private Limited implements various procedures and processes to control access to the production environment and the supporting infrastructure.
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between Mara Studios Private Limited and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans are tested on a periodic basis.
- Operational procedures supporting the achievement of availability commitments to user entities.

Mara Studios Private Limited establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Mara Studios Private Limited's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed, and how staff is hired.

# Components of the System used to Provide Services

**Infrastructure & Network Architecture**

The production infrastructure for the Locus software application is hosted on third-party hosting provider.

Locus software application uses a virtual and secure network environment on top of infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a Virtual Private Cloud (VPC) and accompanying firewall on the infrastructure provider. Locus software application ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

**Software**

Mara Studios Private Limited is responsible for managing the development and operation of the Locus platform including infrastructure components such as servers, databases, and storage systems. The in-scope Locus infrastructure and software components are shown in the table below:

| Primary Infrastructure and Software | |
|---|---|
| **System / Application** | **Business Function / Description** |
| Locus Application | Access to the Locus Saas application is through a web/mobile interface and user authentication. |
| IAM | Identity and access management console for Mara Studios Private Limited’s resources. |
| Firewalls | Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic. |
| Version control system | Source code repository, version control system, and build software. |
| Email | Identity/Email provider for all Mara Studios Private Limited employees. |

**People**

Mara Studios Private Limited's staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel have also been assigned to the following key roles:

**Senior Management:** Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization’s mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and

mitigates IT-related mission risks.

**Information Security Officer:** The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

**Compliance Program Manager:** The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

**System Users:** The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

**Procedures and Policies**

Formal policies and procedures have been established to support the Locus software application. These policies cover:

- Code of Conduct
- Customer Data Deletion
- Information Security
- Third Party Security and Privacy
- Physical and Environmental Security
- Security and Privacy Risk Management
- Information Assets
- Incident Management
- System Protection
- Business Continuity and Disaster Recovery
- Information Classification
- Information System Access control
- Acceptable Use of Information System
- Operation Security

Via the Sprinto platform, all policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

Mara Studios Private Limited also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the Locus software application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

**Data**

Data, as defined by Mara Studios Private Limited, constitutes the following:

- Transaction Data
- Electronic Interface Files
- Output Reports
- Input Reports
- System Files
- Error Logs

All data that is managed, processed and stored as a part of the Locus software application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization. All data is to be assigned one of the following sensitivity levels:

| Data Sensitivity | Description | Examples |
|---|---|---|
| Customer Confidential | Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements.<br><br>Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need. | • Customer system and operating data.<br>• Customer PII.<br>• Anything subject to a confidentiality agreement with a customer. |
| Company Confidential | Information that originated or is owned internally or was entrusted to Mara Studios Private Limited by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public. | • Mara Studios Private Limited's PII.<br>• Unpublished financial information.<br>• Documents and processes explicitly marked as confidential.<br>• Unpublished goals, forecasts, and initiatives marked as confidential.<br>• Pricing/marketing and other undisclosed strategies. |
| Public | Information that has been approved for release to the public and is freely shareable both internally and externally. | • Press releases.<br>• Public website. |

Further, all customer data is treated as confidential. The availability of this data is also limited by job function. All customer data storage and transmission follow industry-standard encryption. The data is also regularly backed up as documented in the Data Backup Procedure evidenced within Operation Security Policy and Procedure.

**Physical Security**

The in-scope system and supporting infrastructure are third-party hosting provider. As such, they responsible for the physical security controls of the in-scope system. Mara Studios Private Limited reviews the SOC 2 report provided by its provider on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the Locus software application.

**Logical Access**

The Locus software application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

Mara Studios Private Limited has identified certain systems that are critical to meet its service commitments. All-access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role-based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assessing the appropriateness of the access and permission levels and making modifications based on the principle of least privilege, whenever necessary.

Access to critical systems requires Multi-Factor Authentication (MFA) wherever possible. Staff members must use complex passwords, wherever possible, for all of their accounts that have access to Mara Studios Private Limited customer data. Staff are encouraged to use passwords that have at least 10 characters, are randomly generated, alphanumeric, and are special-character based. Password configuration settings are configured on each critical system. Additionally, company-owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

**Change Management**

A documented Change Management Procedure evidenced within Operation Security Policy and Procedure guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the Locus system are reviewed, deployed, and managed. The policy covers all changes made to the Locus software application, regardless of their size, scope, or potential impact.

The Change Management Procedure evidenced within Operation Security Policy and Procedure is designed to mitigate the risks of:

- Corrupted or destroyed information.
- Degraded or disrupted software application performance.
- Productivity loss.
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the Locus software application can be initiated by a staff member with an appropriate role.

The ability to implement changes in the production infrastructure is restricted to only those individuals who requires the ability to implement changes as part of their responsibilities.

**Incident Management**

Mara Studios Private Limited has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact Mara Studios Private Limited via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

**Availability**

Mara Studios Private Limited has a documented Business Continuity Plan (BCP) and testing performed against the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

**Asset Management (Hardware and Software)**

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. Mara Studios Private Limited uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

**Vulnerability Management and Penetration Testing**

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk ranked to prioritize the remediation of discovered vulnerabilities.

**Endpoint Management**

Endpoint management solutions are in place that includes policy enforcement on company-issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include but are not limited to enabling screen lock, OS updates, and encryption at rest on critical devices/workstations.

**Boundaries of the System**

The scope of this report includes the Locus software application. It also includes the people, processes, and IT systems that are required to achieve our service commitments toward the customers of this application.

Mara Studios Private Limited depends on a number of vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors. The management understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.

# Complementary Customer Controls

Mara Studios Private Limited's controls related to Locus cover a subset of overall internal control for each user of the software application. The control objectives related to Locus cannot be achieved solely by the controls put in place by Mara Studios Private Limited; each customer's internal controls need to be considered along with Mara Studios Private Limited's controls. Each customer must evaluate its own internal control to determine whether the identified complementary customer controls have been implemented and are operating effectively.

| Complementary Customer Control List | Related Criteria |
|---|---|
| Customers are responsible for managing their organization's Infraon account as well as establishing any customized security solutions or automated processes through the use of setup features. | CC5.1, CC5.2, CC5.3, CC6.1 |
| Customers are responsible for ensuring that authorized users are appointed as administrators for granting access to their Locus software application account. | CC5.2, CC6.3 |
| Customers are responsible for notifying Mara Studios Private Limited of any unauthorized use of any password or account or any other known or suspected breach of security related to the use of Locus software application. | CC7.2, CC7.3, CC7.4 |
| Customers are responsible for any changes made to user and organization data stored within the Locus software application. | CC8.1 |
| Customers are responsible for communicating relevant security and availability issues and incidents to Mara Studios Private Limited through identified channels. | CC7.2, CC7.3, CC7.4 |

# Complementary Subservice Organization Controls

Mara Studios Private Limited uses subservice organizations in support of its system. Mara Studios Private Limited's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Mara Studios Private Limited to be achieved solely by Mara Studios Private Limited. Therefore, user entity controls must be evaluated in conjunction with Mara Studios Private Limited's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below. Mara Studios Private Limited periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC reports.
- Regular meetings to discuss performance.
- Non-disclosure agreements.