samsara
Operate Smarter™

General Customer Responsibility Matrix

April 2025

AREA	SAMSARA	CUSTOMER	CLOUD PROVIDER
 **PLATFORM SECURITY**	1. Implementation of strong authentication protocols, including multi-factor authentication and SSO, and restricted access based on roles and legitimate business needs. Samsara also conducts regular security audits, risk assessments, and vulnerability scanning to maintain a secure platform. 2. Provides comprehensive logging and real-time monitoring, multi-factor authentication, role-based access controls, and SSO integrations. Performs ongoing compliance reviews to protect customer data through annual audits, penetration testing, vulnerability scanning, and proactive measures such as up-to-date patches, antivirus, and intrusion detection/prevention systems. 3. Provide instructions and documentation for configuring SSO with different IdPs. a. While Samsara officially supports Microsoft Entra and Okta as IdPs, other SAML 2.0 providers can be used. Customers can test unverified IdPs by creating a SAML connection in the Samsara dashboard. b. Customers can choose to set up SSO for drivers and administrators separately. This allows for different access controls for each user group.	N/A	Infra

AREA	SAMSARA	CUSTOMER	CLOUD PROVIDER
 **NETWORK SECURITY**	1. Secure the cloud environment and network traffic by utilizing VPC configurations, intrusion detection technologies, and traffic filtering to minimize exposure and block malicious domains, sources, and related content. 2. Secure networking between Samsara components customer data. This includes continuous intrusion detection/prevention (e.g., AWS GuardDuty), traffic filtering from employee endpoints, and leveraging AWS VPC configurations to limit exposure of critical infrastructure. 3. Currently provides direct support for IPv4. a. Explore future support for additional protocols (e.g. IPv6) based on customer demand and industry trends.	Adhere to security best practices, such as using allowlists and the principle of least privilege, in network configuration. If your network environment primarily utilizes IPv6, you may need to implement appropriate translation technologies (such as base 64 proxies or DNS64 and NAT64) to ensure compatibility with Samsara's current IPv4 support. Configure Wi-Fi Hotspot: • Set a unique password for the hotspot. • Limit knowledge of the password to essential personnel to minimize unauthorized usage. • Manage Wi-Fi Data Usage: • Monitor Wi-Fi data usage (refer to Samsara documentation for instructions). • Consider purchasing additional data plans if needed (contact Samsara Sales Representative).	Secure the networking layer.

AREA	SAMSARA	CUSTOMER	CLOUD PROVIDER
 **IAM**	1. Adheres to the principle of least privilege by limiting data access based on roles and job responsibilities, enforcing strong password policies, and implementing secure authentication protocols like SSO and SAML 2.0. 2. Adopt industry-standard best practices and follow the principle of least privileged access. This includes enforcing role-based access controls for employee data access, comprehensive logging and monitoring of all activity, and robust authentication measures (e.g., SSO via Okta, SAML 2.0 integration, and NIST 800-63B-aligned password policies). 3. Offer clear documentation and guidance on managing user roles and permissions by utilizing the following roles effectively. 4. Samsara reserves the right to enforce security controls as needed to protect Samsara and our customers. Samsara has configured the control(s) by default as they are aligned with industry best practices and standards (e.g. NIST, ISO, etc.).	Implement Samsara system controls that are aligned with industry best practices and standards. In the event that your organization wants to temporarily opt out of any enforced controls, please open a support ticket. Utilize strong passwords, multi-factor authentication (MFA), and regular access reviews, employ the principle of least privilege. Leverage organization-level and tag-level access controls to restrict access to specific data and functionalities.	Secure the underlying IAM infrastructure.
 **DATA SECURITY**	1. Encrypt data at rest using FIPS 140-2 compliant standards and in transit with TLS 1.2, AES256 encryption, and signatures. Secure the access channel to the external data source and ensure that customer data is not leaked while being accessed. Provide comprehensive access history, query history, and account usage views with access control and policy-based objects to enable least-privileged access to data. Maintain compliance with data deletion privacy laws and contractual agreements. 2. Samsara encrypts customer data at rest (FIPS 140-2 compliant) and in transit (TLS 1.2) while enforcing strict access controls and monitoring to limit data access to authorized personnel.	Manage data retention and initiate data deletion according to their policies. Manage data classification and access. Use Samsara's provided features in the platform to support data governance as defined in customer policies.	AWS manages physical security for our data center.

AREA	SAMSARA	CUSTOMER	CLOUD PROVIDER
 **INFRA / HIGH AVAILABILITY**	1. Leverage Amazon Web Services (AWS) infrastructure which has SOC 2 Type II attestation, ISO 27001 certification, and FedRAMP authorization. Conduct regular risk assessments and business impact analyses (BIA) to ensure business continuity and disaster recovery. Implement Network Time Protocol (NTP) for accurate timekeeping and security monitoring. Maintain a segregated production environment from the development environment. 2. Leverages AWS's SOC 2 Type II, ISO 27001, and FedRAMP-compliant infrastructure, employing the AWS Shared Responsibility Model to ensure secure, highly available operations. Maintain a segregated production environment, conduct regular risk assessments and BIAs (including backup and restoration testing), and use NTP for synchronized logging—enabling robust business continuity and disaster recovery.	N/A	Secure the infra that supports multiple AZs.
 **APPLICATION SECURITY**	1. Maintain application security through code analysis, credential management, secure development training, and a secure software development lifecycle (SDLC) process. Maintain a comprehensive vulnerability and patch management program. 2. Performs code analysis (manual, static, and dynamic), secure SDLC practices (including OWASP Top 10 training, peer-reviewed commits, in-toto supply chain integrity, and automated deployment/rollback), robust credential management, and a comprehensive vulnerability and patch management program.	N/A	N/A

AREA	SAMSARA	CUSTOMER	CLOUD PROVIDER
 COMPLIANCE	1. Uphold compliance standards and certifications, and provide features that help support customer compliance with IAM, data security, and network security best practices. 2. Maintain independent, external audits, standards, and certifications, while offering features that align with compliance requirements (e.g., IAM, data security, and network security).	N/A	Maintain independent non-Samsara audit, standards and certifications.
 PRIVACY	1. Maintain transparency regarding data processing practices, including a Privacy Policy (https://www.samsara.com/support/privacy), Data Protection Addendum (https://www.samsara.com/legal/data-protection-addendum) and subprocessors list. Provide product features and functionality that enable the use of Samsara products in a way that supports customer compliance with privacy laws and regulations. 2. Maintain privacy program standards and certifications, enabling customers to comply with privacy requirements and best practices.	1. Leverage Samsara's features to meet applicable laws, regulations, and industry best practices that apply to the customer. 2. Identify, conduct, and implement applicable risk assessments, policies, notices, etc. necessary to meet the customer's specific privacy and compliance requirements.	Maintain independent third party audit, standards and certifications.

AREA	SAMSARA	CUSTOMER	CLOUD PROVIDER
AI	1. For Samsara owned and managed AI, follow industry best practices. 2. All uses must comply with Samsara Code of Conduct, Acceptable Use Policy, and other company policies in addition to following industry best practices.	Follow customer own policies and procedures for use of AI.	N/A
DRIVER MANAGEMENT	1. Provide a platform for managing driver documents. 2. Offer pre-defined document templates for common document types.	Manage Driver Documents: • Upload required driver documents (e.g., Accident, Bill of Lading, Citation).	N/A
NOTIFICATIONS & ALERTS	N/A	Configure Alert Triggers: • Define specific events or conditions that trigger alerts (e.g., speeding, engine fault, unauthorized login).	N/A

samsara
Operate Smarter™

Disclaimer

Samsara encourages customers to refer to the guidelines outlined in this document when configuring their environments. This document is provided for informational purposes only and does not modify the Samsara Terms of Service, which shall govern in the event of any conflict. It is the customer's sole responsibility to ensure that all necessary actions are taken to meet their applicable compliance requirements for their systems, including, but not limited, to the recommendations outlined in this document. Samsara is not liable for any failure, breach, or adverse impact arising from the customer's failure to meet these requirements.