A-LIGN

Loadsmart, Inc.

Type 2 SOC 3

2024

loadsmart

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

April 1, 2024 to December 31, 2024

Table of Contents

SECTION 1

ASSERTION OF LOADSMART, INC. MANAGEMENT

ASSERTION OF LOADSMART, INC. MANAGEMENT

January 10, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within Loadsmart, Inc.'s ('Loadsmart' or 'the Company') Transportation, Logistics, Supply Chain, and Storage Services System throughout the period April 1, 2024 to December 31, 2024, to provide reasonable assurance that Loadsmart's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security, Availability, and Confidentiality (applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Loadsmart, Inc.'s Description of Its Transportation, Logistics, Supply Chain, and Storage Services System throughout the period April 1, 2024 to December 31, 2024" 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 April 1, 2024 to December 31, 2024, to provide reasonable assurance that Loadsmart's service commitments and system requirements were achieved based on the Trust Services Criteria. Loadsmart'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 "Loadsmart, Inc.'s Description of Its Transportation, Logistics, Supply Chain, and Storage Services System throughout the period April 1, 2024 to December 31, 2024".

Loadsmart uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Loadsmart, to achieve Loadsmart's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Loadsmart's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Loadsmart's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Loadsmart's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents the applicable Trust Services Criteria and the complementary user entity controls assumed in the design of Loadsmart's controls.

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 April 1, 2024 to December 31, 2024 to provide reasonable assurance that Loadsmart's service commitments and system requirements were achieved based on the applicable Trust Services Criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Loadsmart's controls operated effectively throughout that period.

Amir Mirza

Amir Mirza
CFO
Loadsmart, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

A-LIGN

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Loadsmart, Inc.

Scope

We have examined Loadsmart's accompanying assertion titled "Assertion of Loadsmart, Inc. Management" (assertion) that the controls within Loadsmart's Transportation, Logistics, Supply Chain, and Storage Services System were effective throughout the period April 1, 2024 to December 31, 2024, to provide reasonable assurance that Loadsmart's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security, Availability, and Confidentiality (applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA *Trust Services Criteria*.

Loadsmart uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Loadsmart, to achieve Loadsmart's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Loadsmart's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Loadsmart's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Loadsmart, to achieve Loadsmart's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Loadsmart's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of Loadsmart's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Loadsmart 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 Loadsmart's service commitments and system requirements were achieved. Loadsmart has also provided the accompanying assertion (Loadsmart assertion) about the effectiveness of controls within the system. When preparing its assertion, Loadsmart 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 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 the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its 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.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination 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 are achieved based on the applicable Trust Services Criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 Loadsmart's Transportation, Logistics, Supply Chain, and Storage Services System were suitably designed and operating effectively throughout the period April 1, 2024 to December 31, 2024, to provide reasonable assurance that Loadsmart's service commitments and system requirements were achieved based on the applicable Trust Services Criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Loadsmart's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Loadsmart's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Loadsmart, user entities of Loadsmart's Transportation, Logistics, Supply Chain, and Storage Services System during some or all of the period April 1, 2024 to December 31, 2024, business partners of Loadsmart subject to risks arising from interactions with the Transportation, Logistics, Supply Chain, and Storage Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Tampa, Florida
January 10, 2025

SECTION 3

LOADSMART, INC.'S DESCRIPTION OF ITS TRANSPORTATION, LOGISTICS, SUPPLY CHAIN, AND STORAGE SERVICES SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2024 TO DECEMBER 31, 2024

OVERVIEW OF OPERATIONS

Company Background

Loadsmart was founded in 2014 by Felipe Capella and Ricardo Salgado with the objective of transforming the logistics landscape by leveraging modern technology and industry expertise to deliver optimized, reliable, and transparent freight services and solutions. The company is currently based in Chicago, Illinois.

From digital freight brokerage and consultancy to software tools, Loadsmart empowers shippers, carriers, and warehouses to move more with less-increasing efficiency, reducing costs, and enhancing service quality. This led Loadsmart to achieve several awards throughout the past years, including the “Best Newcomer” at the Customer Excellence Awards 2023.

Description of Services Provided

Loadsmart is a logistics services and solutions provider offering a digital brokerage, freight procurement tools, dock scheduling software, truck management software, managed transportation services, freight and network optimization, and custom solutions that operate globally.

Loadsmart’s Alice application is an internal Transportation Management System (TMS). It is used only by People affiliated with Loadsmart. Employees and/or independent contractors - herein “Loadies” - and its Application Programming Interfaces (APIs) are used by other services such as Loadsmart’s Carrier Loadboard and ShipperGuide TMS. Inside Alice, the representatives manage the full lifecycle of a load.

Loadsmart’s Carrier Loadboard is a carrier portal used to review loads to be moved on Loadsmart’s ecosystem. Carriers have access to different loads, can accept them, and follow the full lifecycle of the load.

Loadsmart’s CarrierTMS (sometimes also referred to as Kamion) is an easy to use, turnkey carrier truck management solution that drives profitability for carriers and private fleets through optimizing dispatch, load management, document management, reporting, and invoicing. CarrierTMS also connects carriers to an agnostic marketplace of loads, services, factoring, and integrations to support fleets of every size.

Loadsmart’s Opendock is a dock scheduling software that improves operations at facilities receiving inbound shipments or sending outbound shipments. Dock appointment scheduling helps configure facilities, load types, dock doors, capacity, and labor to determine appointment availability.

Loadsmart’s ShipperGuide TMS is a cost-effective, intuitive planning, procurement, and execution platform to manage request for proposals (RFPs), spot procurement, set tender guidelines, and track freight with carriers. The platform reduces annual freight costs by providing AI insights on price forecasts, real-time and historical pricing comparisons, and lane data - leveraging large language model (LLM) interactions. Customers could easily find spot rates for modes such as Full Truckload (FTL), Less-than-Truckload (LTL), volume Less-than-Truckload (vLTL), Intermodal, and Drayage.

The brokerage department handles FTL, LTL, Partial Truckload (PTL), Drayage, Expedited and Intermodal freight, ensuring quality service. Features include:

- Instant pricing
- Spot API Ratings into other TMS
- Dynamic Contracts that adjust to market conditions
- Booking and Tracking platform
- 24/7 support of freight specialists

Principal Service Commitments and System Requirements

Loadsmart designs its processes and procedures related to security, confidentiality and availability to meet its objectives for its digital brokerage, freight procurement tools, dock scheduling software, truck management software, managed transportation services, freight and network optimization, and custom services. Those objectives are based on the service commitments that Loadsmart makes to user entities, the laws and regulations that govern the provision of aforementioned mentioned services, and the financial, operational, and compliance requirements that Loadsmart has established for the services. The digital brokerage, freight procurement tools, dock scheduling software, truck management software, managed transportation services, freight and network optimization, and custom services of Loadsmart are subject to the security and privacy requirements of applicable state privacy security laws and regulations in the jurisdictions in which Loadsmart operates.

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

Security principles within the fundamental designs of the security, confidentiality and availability 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.

Loadsmart establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Loadsmart'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 business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the security, confidentiality and availability.

Components of the System

Infrastructure

Primary infrastructure used to provide Loadsmart's Transportation, Logistics, Supply Chain, and Storage Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Kubernetes Nodes	AWS Elastic Compute Cloud (EC2)	Hosts the Kubernetes nodes
Databases	AWS Relational Database Service (RDS), OpenSearch	Manages PostgreSQL databases and Elasticsearch
Network Address Translation (NAT) Gateways	AWS NAT Gateway	Manages NAT Gateways
API Gateway	AWS API Gateway	Manages API Gateways
Cloud Provider	AWS	Hosts cloud-based solutions

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Kubernetes Clusters	AWS Elastic Kubernetes Service (EKS)	Manages Kubernetes clusters

Software

Primary software used to provide Loadsmart's Transportation, Logistics, Supply Chain, and Storage Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
AWS	Amazon Linux CentOS Ubuntu Bionic 18.04 Ubuntu Xenial 16.04 Windows	Hosts cloud-based solutions
Datadog	N/A	Monitoring and alerting system
Google Workspace	N/A	Email and cloud storage (Google Drive) for documents
Paylocity	N/A	Human resources (HR) information system
Sentry	N/A	Performance monitoring
GitHub	N/A	Code repository, versioning control and security tools
Teleport	N/A	Manage access to servers and databases
Okta	N/A	Internal identity manager
Atlassian (Confluence and Jira)	N/A	Tickets tracking (Jira) and documentation (Confluence)
Zendesk	N/A	Help desk ticketing system

People

Loadsmart has a staff of approximately 500 employees organized in the following functional areas:

- Corporate: Chief Executive Officer (CEO), Chief Technology Officer (CTO), CFO, and Vice Presidents (VPs) of Shipper Solutions and of Software Solutions
- Legal: the legal department reports to Loadsmart's CEO and is headed by the Director of Legal and Compliance. It is responsible for legal matters within the company but focuses primarily on corporate law
- Engineering: Under the CTO, there is the Engineering department, which includes:
    - Product engineering teams
    - Agile team
    - Platform: Site reliability engineers (SREs) + Security + Information Technology (IT) Operations
    - Data Engineering

- Finance: Under the CFO, divides itself into Pricing Strategy, Financial, Accounting, Revenue Operations:
    - People and Experiences is also under the CFO at this moment
- Product: Under a VP of Product, Loadsmart has the Product department which includes Product Design and Product Management for the applications
- Operations: Focused on how to connect Shippers to Carriers. There are different areas such as:
    - Carrier operations
    - Carrier procurement
    - Capacity development
    - LTL and specialized services
- Sales: Loadsmart has different sales areas depending on where inside the freight cycle their activity is located:
    - Enterprise Accounts Sales
    - Shipper Solutions
    - Brokerage Sales

Data

Data will vary depending on the product or service provided:

Alice

- Input: shippers, carriers, docs, facilities, pick-up and delivery data. Shipment, tracking data, accounting, margins, contract.
- Output: full status of the shipment lifecycle.

Carrier Loadboard

- Input: Availability, routes, pick-up and delivery dates, evidence of delivery, documents.
- Output: visibility of the load, tracking, notifications, documentation and invoicing.

CarrierTMS (Kamion)

- Input: private fleets data, marketplace of loads, factoring, people management and integrations.
- Output: analytics, strategy reports, performance reports, financial reports.

Opendock

- Input: facilities, load types, dock doors, capacity, and labor to determine appointment availability.
- Output: schedules, appointments, reports, maps.

ShipperGuide

- Input: shippers, pick-up and delivery data. Shipment, tracking data, accounting, margins, contracts, RFP.
- Output: full status of the shipment lifecycle, contract information, history.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to the Loadsmart policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Loadsmart team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope service.

Logical Access

Loadsmart uses Okta to manage their internal identities inside their ecosystem. It is used as authentication method to the most critical internal and infrastructure services:

- AWS
- Engineering Virtual Private Network (VPN)
- Email and document repository (Google Workspaces and Drive)
- Alice

When considering Engineering, Loadsmart also leverages GitHub as an authentication method to access specific resources:

- Kubernetes clusters
- Databases

Multifactor authentication (MFA) is required for both authentication methods.

In general, a position is created on the HR system - right now Paylocity. It synchronizes with Okta and the person already inherits a basic set of permissions. For Engineering, because of its critical accesses, the creation needs to be made manually by IT. IT also has specific automations to create and manage users when needed.

Whenever a person is terminated, HR sends a communication to resource owners and the users are blocked immediately on Okta and it spreads through other Okta services. Once again, IT has automations that are responsible for blocking users directly on specific systems.

On a quarterly basis, Security reviews critical accesses to make sure users have been properly offboarded and/or shifted to their current permission set accordingly. There are also extraordinary situations in which an access review is required e.g., the company went through a reduction in force and engineering restructuring last year which was finalized in 2024.

Computer Operations - Backups

The in-scope applications are cloud based, Loadsmart leverages AWS automated backup mechanisms to perform backups. They are performed to multi-availability zones, multi-region datacenters and Loadsmart has also defined a cross-account backup as a third measure in case of a critical emergency.

Loadsmart has monitoring and alerts in place in case a backup fails and checks to verify if a backup was done in the past 25 hours as a secondary verification point.

Computer Operations - Availability

Loadsmart has a robust incident response policies and procedures in place. These provide a clear framework for personnel to quickly identify, report, and effectively respond to any IT incidents, including unavailability, potential system security breaches or application-related issues.

Loadsmart uses Datadog to receive logs and metrics from different sources in order to monitor and alert in case of any anomaly. Some of the sources are:

- AWS CloudTrail
- AWS EKS
- AWS RDS

- AWS Web Application Firewall (WAF)
- AWS GuardDuty
- AWS API Gateway
- Okta
- 1Password
- GitHub

Change Control

Loadsmart has a well-defined Systems Development Life Cycle (SDLC) with comprehensive policies and procedures. These ensure consistent change control across application and infrastructure development, including request initiation, documentation, testing, and approval processes. With the exception of emergency changes, no code is published to production without a resource owner's approval. In the case of an emergency, the team has 20 days to implement it following the appropriate paths and channels and/or to approve it afterwards.

GitHub is used as the main resource to track code and infrastructure changes, allowing to review, approve and monitor any change implemented to the ecosystem.

Loadsmart also configured GitHub to make sure the controls stay in place without any unexpected changes to it. Finally, GitHub logs are sent to Datadog, so the appropriate personnel are alerted whenever a policy is not followed.

Data Communications

Loadsmart has different AWS accounts following the AWS Control Tower directive to manage the organization properly. Product accounts are fully managed using Terraform as the infrastructure as code language of choice. With it Loadsmart can track and monitor changes preserving the integrity and security of the in-scope accounts.

By default, Loadsmart uses multi availability zones and multi regions whenever possible to ensure redundancy if an error occurs.

In order to connect to databases and applications, users need to be connected to the Engineering VPN, which uses Okta with MFA to manage access but also GitHub (with mandatory MFA as well).

Boundaries of the System

The scope of this report includes Loadsmart’s Transportation, Logistics, Supply Chain, and Storage Services System performed in the Chicago, Illinois facility.

This report does not include the cloud hosting services provided by AWS at multiple facilities.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization’s last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization’s last review.

Criteria Not Applicable to the System

All Common Criteria/Security, Availability, and Confidentiality criteria were applicable to the Loadsmart Transportation, Logistics, Supply Chain, and Storage Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS for the Transportation, Logistics, Supply Chain, and Storage Services System.

Subservice Description of Services

AWS provides cloud hosting services, which includes implementing physical security controls to protect the housed in-scope systems. Controls include, but are not limited to, visitor sign-ins, required use of badges for authorized personnel, and monitoring and logging of the physical access to the facilities.

Complementary Subservice Organization Controls

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

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:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units (unless maintained by Amazon), and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.
		UPS units provide backup power in the event of an electrical failure in Amazon-owned data centers and third-party colocation sites where Amazon maintains the UPS units.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.
		RDS Specific - If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point in-time recovery.

Loadsmart 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 SLA. In addition, Loadsmart performs monitoring of the subservice organization controls, including reviewing attestation reports over services provided by vendors and the subservice organization.

COMPLEMENTARY USER ENTITY CONTROLS

Loadsmart'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 of the Trust Services Criteria related to Loadsmart's services to be solely achieved by Loadsmart control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Loadsmart.

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 Loadsmart.

2. User entities are responsible for the supervision, management, and control of the use of Loadsmart services by their personnel.
3. User entities are responsible for developing their own disaster discovery, Business Continuity Plans (BCPs), and incident response.
4. User entities are responsible for managing users inside their accounts for applicable Loadsmart products.
5. User entities are responsible for notifying Loadsmart for any suspicious activity, security breaches, and the like.