# SOC 3 Report

HI-TOUCH ON THE GO

## Report on Nation Safe Drivers - Insurance and Automotive Related Products Relevant to Security

Throughout the Period 3/6/2024 to 10/21/2024

*SOC 3® - SOC Service Organizations: Trust Services Criteria for General Use Report*

Sensitive: The information in this document is not to be disclosed outside of Nation Safe Drivers or Strike Graph Inc. without the prior written consent of both organizations.

# TABLE OF CONTENTS

SECTION I - Service Organization Management's Assertion 2

SECTION II - Independent Service Auditor's Report 3

Attachment A - Description of the Boundaries of Service Organization's System 5

Attachment B – Principal Service Commitments and System Requirements 6

# SECTION I - Service Organization Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Nation Safe Drivers - Insurance and Automotive Related Products (system) throughout the period 3/6/2024 to 10/21/2024, to provide reasonable assurance that Nation Safe Drivers's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period 3/6/2024 to 10/21/2024, to provide reasonable assurance that Nation Safe Drivers'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 (AICPA, Trust Services Criteria). Nation Safe Drivers'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 attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period 3/6/2024 to 10/21/2024, to provide reasonable assurance that Nation Safe Drivers's service commitments and system requirements were achieved based on the applicable trust services criteria.

NSD
HI-TOUCH ON THE GO

Michael Sothen

**Michael Sothern,** CFO
Nation Safe Drivers
11.13.2024

# SECTION II - Independent Service Auditor's Report

## To: Nation Safe Drivers's Management Team

### Scope

We have examined management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of Its Controls Over the Nation Safe Drivers - Insurance and Automotive Related Products Based on the Trust Services Criteria for Security (Assertion), that Nation Safe Drivers's controls over the Nation Safe Drivers - Insurance and Automotive Related Products (System) were effective throughout the period 3/6/2024 to 10/21/2024, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to Security (applicable trust services criteria) set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

### Management Responsibilities

Nation Safe Drivers's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Nation Safe Drivers - Insurance and Automotive Related Products and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- identifying, designing, implementing, operating, and monitoring effective controls over the Nation Safe Drivers - Insurance and Automotive Related Products to mitigate risks that threaten the achievement of the principal service commitments and system requirements

### Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes (1) obtaining an understanding of Nation Safe Drivers's relevant Security, policies, processes, and controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Nation Safe Drivers's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

### Inherent Limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Nation Safe Drivers's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

## Opinion

In our opinion, Nation Safe Drivers's controls over the system were effective throughout the period 3/6/2024 to 10/21/2024, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Amjad Abu Khamis

**Amjad Abu Khamis**
License Number: 08224
11.13.2024

Sg Strike Graph

# Attachment A - Description of the Boundaries of Service Organization’s System

## Company Background

Nation Safe Drivers (NSDs) was established in 1962 and is based in Boca Raton, FL. For the last 60 years Original Equipment Manufacturers (OEMs), dealerships, tire manufacturers, car rental companies, and others have relied on NSDs expertise in mobile networks and claims administration to deliver best in class customer experiences. With strategically located call centers in the United States and Canada, NSD provides services 24-hours a day 7 days a week, and 365 days a year. NSD’s HQ is in Boca Raton, Florida with multiple call center locations in the United States and around the world.

NSD’s mission is to provide the industry’s best products and services that deliver exceptional benefits and value with a best-in-class customer experience.

## Overview of the System

NSD serves Automotive Dealerships and Manufacturers, Standard and Non-standard Insurance Carriers and Agencies, Rental Car Companies, Power Sports, Tire Manufacturers and Distributors, and Financial Lenders, Banks, and Credit Unions.

## Key Features of the Qore System

Nation Safe Drivers’ QORE platform is comprised of the following key features:

- **Dispatching** – This feature allows the dispatching of towing service to be executed.
- **Client** – This feature gives clients the ability to review all interactions with NSD in the areas of dispatching and claims.

## Principle Service Commitments and System Requirements

Nation Safe Drivers has designed its processes and procedures related to the Qore Applications (or the “System”) to meet its objectives for its Roadside Assistance (“Services”). Those objectives are based on the service commitments that Nation Safe Drivers makes to its user entities and the operational and compliance requirements that it has established for the services. These commitments also take into consideration the law and regulations in the jurisdictions in which Nation Safe Drivers services are offered.

Nation Safe Drivers establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in NSD's system policies and procedures, system design documents, 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.

This report is limited in scope to the Security Trust Services Criteria based on guidance from the AICPA. The controls that management has identified to meet each criterion is described in detail within the ‘Control Environment’ section of this System Description as well as in Section 4 of this report. They are not included here to eliminate the redundancy that would result from listing them in this section. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of NSD’s description of the system. Any applicable trust services criteria that are not addressed by control activities at Nation Safe Drivers are described within the 'Complementary Subservice Organization Controls' section below.

NSD's principal service commitments and system requirements are:

| Trust Services Criteria | Service Commitments | System Requirements |
|---|---|---|
| Security | ● The Business will employ administrative, physical, and technical measures in accordance with applicable industry practices to protect the System and prevent the accidental loss or unauthorized access, use, alteration, or disclosure of ePHI under its control during each order term.<br>● All data transmitted between the Company and the user of the system is protected using transport layer security (TLS) and HTTP strict Transport Security.<br>● Access to environments that contain customer data requires a series of authentication and authorization controls, including multi-factor authentication (MFA).<br>● The Business  monitors critical infrastructure for security related events by using a custom implementation of open source and commercial technologies. | ● Employee provisioning and deprovisioning standards<br>● Logical access controls such as user IDs and passwords to access the System.<br>● Encryption of data in transit over public networks<br>● Security monitoring controls |

## System Components

The Qore platform is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of this system description is to delineate the boundaries of the system, which includes the services outlined above and the following components, described below: people, data, infrastructure, software, and procedures.

### People

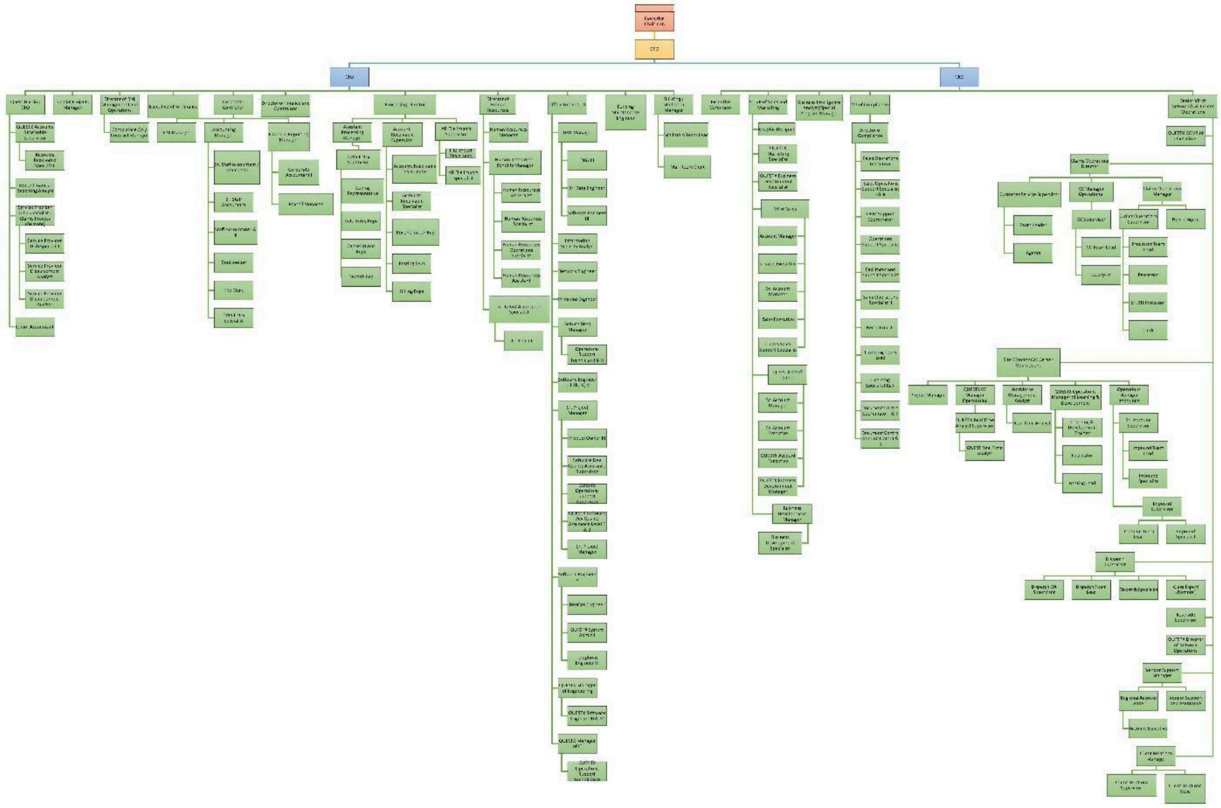
Nation Safe Drivers is organized into sixteen functional areas. Within the sixteen functional areas, organizational and reporting hierarchies have been defined where the Functional area department heads report to the Chief Financial Officer (CFO), Chief Operating Officer (COO), Chief Revenue Officer (CRO), Chief Legal Officer (CLO), Chief People Officer (CPO), and Chief Information Technology Officer (CITO) who then report to the Chief Executive Officer The responsibilities for specific roles are clearly defined with job descriptions. The organizational structure provides the framework within which NSD's activities for achieving entity-wide objectives are planned, executed, controlled, and monitored.

NSD's entire organization is engaged in maturing our Information Technology I(IT) Operations and Cyber Security Program. This initiative has the approval of the Executive Team and all the Department Heads that communicate the effort to each department's employees. The Office of the Chief Information Technology Officer (CITO), Human Resources, Building Manager, Legal and Compliance, Processing, Risk Management, Controller, Finance, Special Projects, Quest and the Offices of the CEO and Executive Chairman are all involved in the effort to mature IT Operations and Cyber Security to protect our customers, NSD employees and promote business growth,

The following NSD teams are responsible for evaluating and managing controls and other activities to prevent, detect, mitigate, and remediate system incidents.

- NSD's Executive Leadership is responsible for setting the company's strategic goals and managing company-wide activities.
- The Office of the CITO, Processing Director, Special Projects, and Processing are responsible for developing features and supporting the platform. The Office of the CITO, Executives and Department Heads are responsible for incident management.
- Sales and Marketing is responsible for creating and managing product roadmap.
- Human Resources (HR) is responsible for HR policies, practices, and processes (e.g., talent acquisitions, compensation, employee benefits, employee compliance, onboarding, offboarding and training).

Org Chart All Employees - Organization 5.6.24.pdf

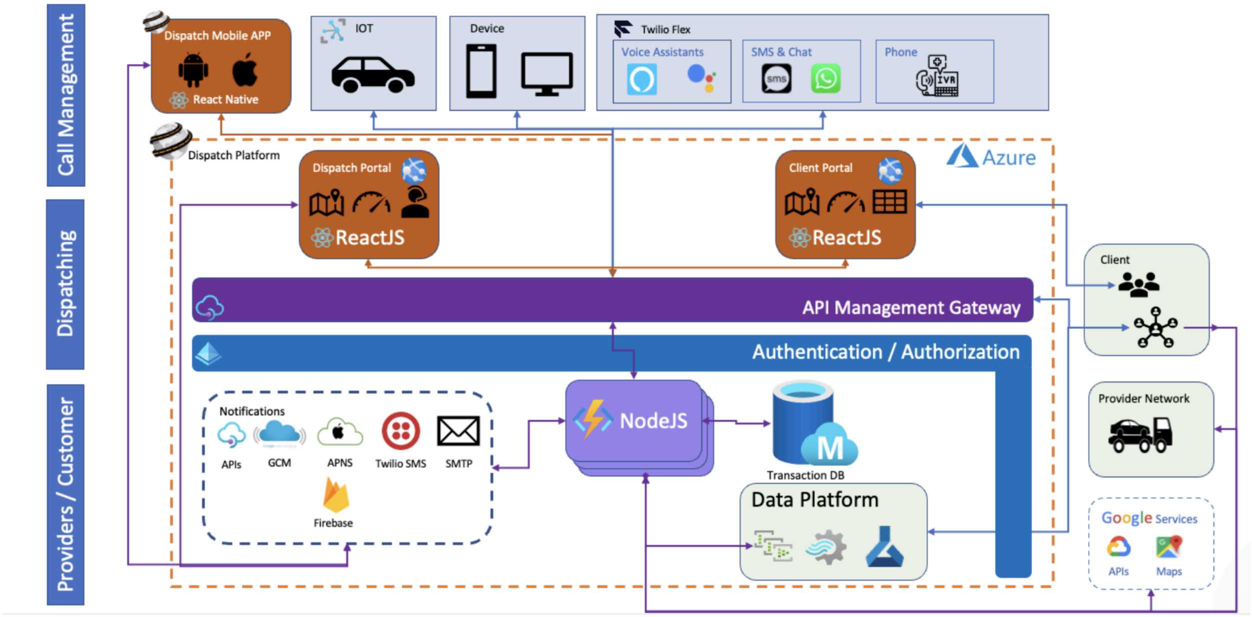


## Data

Nation Safe Drivers separates customer data using a logical permission scheme. Access to data is dependent upon the domain of the user's account that is validated. For example, in this model, all data for the users of the domain nationsafedrivers.com are logically separated from other domains within the System.

Only Nation Safe Drivers authorized personnel have access to production data. To access production data authorized personnel must use a key based SSH tunnel from behind a firewall and into a provided bastion server. All customer data in the system, whether sensitive or standard, is encrypted both at transmission and at rest.

Nation Safe Drivers retains data on a case-by-case basis which is specified in a customer's contract or data retention requirements. If data needs to be destroyed this must be approved by the CITO and a ticket provided for that removal. A backup must be made before any data is destroyed. Then the after-action activity must include a test and review by the customer to see that the data was properly destroyed.


Document valid as of last updated date 9/16/2024

## Third Party Access

No third-party providers have access to NSD data.

## Infrastructure

The primary infrastructure supporting the Qore is comprised of:

| AZURE Computing Infrastructure | | |
|---|---|---|
| Infrastructure | Type | Purpose |
| Azure | Database | Primary production database |
| Azure | Infrastructure | Servers |
| Azure | PaaS | API Gateway, Functions |

## Procedures

Management has developed policies that establish the organization's overall approach to internal controls related to security and operational processes. These policies comply with overall business objectives and are aimed to minimize risk through preventive measures, timely identification of irregularities, limitation of losses, and timely restoration.

The organization has established control activities, based on policies that are conducted through various procedures. These procedures include, but are not limited to:

- Oversight, selection, documentation, implementation and monitoring of security controls.
- Authorization, changes to, and termination of information system access
- Maintenance and support of the security system and necessary backup and offline storage
- Governance and processes for change management
- Incident response guidelines and processes
- Vendor oversight and processes to mitigate vendor risk.
- IT and operational risk management

## Boundaries of the System

The people, data, infrastructure, software, and procedures described above establish the system boundaries for our SOC 2 examination.

## Complementary Subservice Organization Controls

No subservice organization controls are relevant to NSD's Qore System.

# Relevant Aspects of the Control Environment, Risk Assessment, Information and Communications, and Monitoring

## Control Environment

NSD's control environment sets the tone of the organization and influences the control consciousness of its personnel. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications. The control environment includes controls that may have a pervasive effect on the organization, an effect on specific processes, as well as security controls intended to effectively protect client data and provide a stable environment for the security of NSD's client-facing services. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by executive management and operations management.

### Integrity and Ethical Values

Integrity and ethical values are essential elements of NSD's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of NSD's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. Specific control activities that Nation Safe Drivers has implemented in this area are:

- NSD performs Background Checks on all employees.
- NSD provides security training for its employees on an annual basis.
- NSD employees acknowledge the Acceptable Use Policy
- NSDs employee handbook is provided as a guide for ethical behavior.

## Board Management Oversight

NSD's control consciousness is influenced significantly by the participation of its executive team. The executive team meets on a periodic basis to oversee operations management activities and to discuss and monitor related issues. Executive management meets and interacts with team members as a component of day-to-day operations to discuss business objectives and operational issues.

## Organizational Structure

Nation Safe Drivers organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Nation Safe Drivers management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. Nation Safe Drivers is organized along functional areas. Within functional areas, organizational and reporting hierarchies have been defined and responsibilities have been assigned.

## Assignment of Authority and Responsibility

NSD's assignment of authority and responsibility 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 business practices, knowledge and experience of key personnel, and resources provided for performing duties. In addition, it includes policies and communications directed at ensuring that 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.

## Commitment to Competence

Nation Safe Drivers is committed to providing high quality professional and technological resources. This includes management's consideration of the knowledge and skills necessary to accomplish tasks that define each employee's roles and responsibilities. To this end, management has implemented the following:

- Access is provided to users based on their role and responsibility.
- NSD Cyber Security Awareness Training is provided on an annual basis through KnowBe4.
- Annually allocates budget for cyber security initiatives.
- Performs tabletop tests to train staff members about their role in the event of a disaster incident.

## Accountability

Nation Safe Drivers management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, management's attitudes and actions toward financial reporting, and management's attitudes toward information processing, accounting functions and personnel. Management meetings are held frequently to address issues as they are brought to management's attention. NSD' human resources policies and practices relate to employee hiring, orientation, training, evaluation, promotion, compensation, and disciplinary activities. Specific control activities that Nation Safe Drivers has implemented in this area include:

- Requires that all employees considered for employment at NSD pass a background check.
- Requires new hires and existing employees to attend cyber security training on an annual basis.
- Compliance team reviews risks that are reported to NSDs Management and Executive teams.
- Follows Generally Accepted Accounting Principles (GAAP) for financial reporting.

## Controls

### Security Management

Management has developed information security policies and related procedures to govern the security program at NSD. The Information Security Policy is maintained, reviewed, and annually updated by the Chief Information Technology Officer (CITO). The development of an information security program, processes and procedures are the responsibility of the Chief Information Technology Officer (CITO). The Information Security Policies are reviewed and approved annually or as business needs change. Procedure documents related to access control and change management are updated as business needs change.

These policies and procedures cover the following key security life cycle areas:

- Data classification
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response

## Logical and Physical Access

NSD maintains an office at 5600 Broken Sound Blvd, NW, Boca Raton, FL 33487. Access to the offices is secured by key card access and all keycard access is logged. Visitors must be accompanied by an employee to the location for their visit and escorted back to the lobby once that visit is over. Visitors can check-in at the front desk of NSDs lobby. Employees are notified via teams, email, or phone when a visitor has arrived. The building is monitored 24/7, security guards are present, video surveillance is at each entrance and external doors are locked via magnetic lock and can only be accessed with a key card issued to NSD employees or by contacting the front desk through a remote speaker system.

## Change Management

Nation Safe Drivers has a Change Management Policy which governs deliberate changes to the IT environment, including infrastructure, data, and software development. The Change Management policy governs the request, documentation, testing and approval of changes. All technology acquisition, development and maintenance processes are governed by change management procedures. The Change Management Policy is communicated to relevant personnel and updated annually, or as business needs require. The Chief Information Technology Officer (CITO) is the owner of the Change Management Policy and is responsible for ensuring that changes to IT services are made in a manner appropriate to their impact on Company Operations.

Nation Safe Drivers has implemented a SCRUM[1] based software development approach as a change management practice. We design our release roadmap around enhancement releases, minor releases, and major releases. Prioritization is the responsibility of the software engineering manager and product owner.

Nation Safe Driver's software engineering team utilizes Jira to manage specific changes throughout the change control processes. For any system change a change request ticket must be written specifying the change requested.

When tickets have been prioritized, they are matched with a planned software release. A release will include multiple tickets. Enhancement releases are scheduled and can be accomplished quickly when important bug fixes, patches or threats are needed – emergency fix. Minor releases usually

[1] SCRUM is an agile team collaboration framework commonly used in software development and other industries.  SCRUM prescribes for teams to break work into goals to be completed within time-boxed iterations, called sprints.

correspond with a new feature. Major releases can contain multiple features or new products unto themselves.

Weekly Sprint Planning meetings allow the Engineering Manager to assign specific tasks according to the release roadmap. This also provides an important touchpoint for the entire product team. Daily standup meetings with the team allow for quick decisions or questions to be introduced during a sprint.

Executed changes are developed in software code on a separate branch of a project's repository. When an engineer or resource has completed a ticket in their separate branch, they create a "merge request" in the repository. A merge request must be reviewed and approved by a separate engineer or resource. Once the request has been approved, the merge request can be completed, and the software code is included in a development branch within the git repository. The developer branch is automatically deployed via Gitlab CI/CD tools to the development environment on AZURE. This environment allows the product team to execute rapid tests in the completely merged code base on a duplicated server environment.

Once the required tickets for a specific release are completed the development branch is merged to a testing branch. This is executed with the approval of the Engineering Manager. Testing branches are automatically deployed to a testing environment on Azure that is duplicated via terraform to the production environment. This allows the engineering team to execute a complete regression test for a production release.

After a regression test has been completed and the quality of the code approved by the Product Owner a production release can be created. Nation Safe Drivers DevOps team tags the testing branch with a tag that specifies the release number e.g., 1.1.0. This tag is then pushed via command through the CI/CD process registering the code in the Enterprise Container Registry and then deploying those containers to a cluster in the Enterprise Container Service. Product Owners then perform a brief smoke test to ensure that the changes have not resulted in an error. If any roll-back activity is required, the Product Owners will execute that immediately with DevOps.

## Data Backup and Disaster Recovery

All Nation Safe Drivers customer data is considered the highest priority for data retention. Our databases are deployed on the Relational Data Service (RDS) provided by Azure. Our database software provides full ACID compliant transaction support. Every database has an automated data backup and restoration policy. This is coded into Terraform deployment scripts and tested with each major release. Backups are achieved using Azure tools daily and all snapshots are retained for 30 days. Data is backed up following a set schedule; access to backups is restricted to privileged users.

## Incident Response

Nation Safe Drivers relies on Azure incident logging system for incidents impacting the Azure infrastructure. For other incidents, incident response guidelines are published and available to all employees and include definition of an incident, employee responsibilities and notification procedures, and data necessary to analyze an incident to determine impact are documented. A security incident recovery test is performed annually; resulting findings are integrated into the Incident Response Plan ("IRP").

The IRP includes:

- definition of an incident
- employee responsibilities
- notification procedures
- containment
- mitigation plan
- a step to apply patch, fix, restoration of data, or enable new tool setting (such as firewall rules)
- restoration of services

- root cause analysis

A tracking system is in place to centrally maintain, manage, and monitor change requests that result from incidents that require a change to be made. Incident response procedures for all employees are included in the annual security training.

### Vendor Management

Nation Safe Drivers defines vendor management roles, contract expectations and vendor risks in adherence to Vendor Management Policy. The CFO, Risk Management, and Legal Team oversee vendor management. Formal contracts are utilized for vendor and business partner relationships; scope, responsibilities, compliance requirements and service levels (if required) are included in the contracts.

Nation Safe Drivers performs due diligence activities over new vendors prior to contract execution and on an annual basis thereafter. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk. Third party SOC 2 reports are reviewed for impact to the company environment.

### System Monitoring

NSD's system is monitored at both the infrastructure level and the application level. NSD utilizes Arctic Wolf to monitor its infrastructure and applications. Arctic Wolf sends NSD Notifications that are monitored by the IT Team and all alerts, depending on their criticality, will notify appropriate users through a combination of email, Teams messaging.

CrowdStrike is deployed to the information system as our antivirus. NSD headquarters employs a SonicWall firewall solution. BitLocker endpoint protection is deployed to all company issued devices, providing advanced anti-malware/anti-virus and firewall protection, preventing accidental or malicious introduction of issues into our production environment. Outlook settings have been enabled to scan emails for malware & phishing attempts prior to and after email delivery, respectively.

## Information and Communications

Information and communication are integral components of the Nation Safe Drivers internal control system. It is the process of identifying, capturing, and exchanging information in the time frame necessary to conduct, manage and control the entity's operations. At NSD, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, service providers, and employees.

- NSD Management communicates with employees using: E-mail.
- Teams Messaging
- Town Halls
- Annual Training

The IT Team meets weekly to discuss security incidents, alerts, and emerging security issues. Additionally, company wide meetings are held weekly to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. NSD's intranet site includes information employees can reference for data security guidance. Additionally, email and Teams messages are used to communicate time-sensitive information.

NSD has implemented communication structure to help provide assurance that customers understand their roles and responsibilities in processing their data and communication of significant events. This includes a resolute team to communicate time-sensitive information when there are customer impacting security changes. IT will notify customers of maintenance, outages, product releases, security incidents or platform changes that impact security or privacy.

## Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changing conditions. Management has implemented Arctic Wolf to address timely and appropriate responses to issues that may impact information security. Automated systems (ex: IDS, firewall, vulnerability scans, patch alerts) are monitored for security events impacting NSD's systems and remediations are actioned as needed.

In addition, NSD monitors the quality of internal control performance as a normal part of their activities. They are heavily involved in day-to-day activities and regularly review various aspects of internal and customer-facing operations to:

- Determine if objectives are achieved.
- Identify any new risks that develop.
- Implement appropriate measures to address those risks.

The monitoring process is achieved through several ongoing management oversight activities that include:

- Annual Penetration Testing
- Weekly Vulnerability Reporting and Remediation
- Patch Management
- Intrusion Detection and Prevention Alerts

## Risk Assessment

The risk assessment occurs annually, or on as needed basis. It includes risks that could act against the company's objectives and service commitments, as well as specific risks related to a compromise of data security. The level of each identified risk is determined by considering the impact of the risk itself and the likelihood of the risk materializing, and high scoring risks are actioned upon. Risks are analyzed to determine whether the risk meets company risk acceptance criteria to be accepted or whether a mitigation plan will be applied. Mitigation plans include both the individual or department responsible for the plan and may include budget considerations.

Management considers the following in its risk assessment:

- Risks that could impact the security of the organization's IT environment.
- Risk of fraud.
- Vendor or supply chain risks.
- Risks to customer or employee data.
- Cross department risks that may impact security objectives.
- Identification and assessment of changes, such as environmental, regulatory, and technological changes that could significantly affect the system of internal control for security.

## Incidents in the Last 12 Months

There have been no significant incidents related to a control failure  that impacted service commitments or system requirements, which required to be disclosed or had a material impact requiring disclosure.

# Complementary User Entity Controls

NSD's services were designed with the assumption that certain controls would be implemented by the broadest set of user entities. These controls should be in operation at user entities to complement NSD's controls. The user-entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user entities.

User entities are responsible for:

- Ensuring that appropriate user authentication controls are in place.
- Ensuring that access to the client portal is restricted to authorized users and access rights are commensurate with their job responsibilities.
- Ensuring that usernames and passwords for the client portal are not shared and kept confidential.
- Ensuring that access to add, modify, or delete user accounts or roles within the client portal is restricted to appropriate personnel and is authorized.
- Ensuring that changes to contacts at user organizations are communicated in a timely manner.
- Ensuring that data confidentiality requirements and commitments are adhered to in accordance with service level agreements.

# Attachment B – Principal Service Commitments and System Requirements

**Overview**

Commitments are declarations made by management to customers regarding the performance of Nation Safe Drivers - Insurance and Automotive Related Products.

Nation Safe Drivers designs its processes and procedures to meet its objectives for the Nation Safe Drivers - Insurance and Automotive Related Products. Those objectives are based on the service commitments that Nation Safe Drivers makes to user entities (customers), the laws and regulations that govern the provision of the Nation Safe Drivers - Insurance and Automotive Related Products, and the financial, operational and compliance requirements that Nation Safe Drivers  has established for the services.

The Nation Safe Drivers services are subject to relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Nation Safe Drivers operates.

Nation Safe Drivers  agreements and commitments are captured in the following documents:

- Nation Safe Drivers - Cryptographic Controls and Key Management Policy
- Nation Safe Drivers - Acceptable Use Policy
- Nation Safe Drivers - Enterprise Business Continuity Plan

System requirements are specifications regarding how Nation Safe Drivers - Insurance and Automotive Related Products should function to meet Nation Safe Drivers' principal commitments to user entities.

Nation Safe Drivers establishes operational requirements that support the achievement of security, availability and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Nation Safe Drivers'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 Nation Safe Drivers - Insurance and Automotive Related Products.

Nation Safe Drivers's principal service commitments and system requirements related to Nation Safe Drivers - Insurance and Automotive Related Products include the following:

| Trust Services Category | Service Commitments | System Requirements |
|---|---|---|
| **Security** | ● The Company will protect personally identifying information and the security of the information system designed to prevent unauthorized access, use, modification, disclosure, destruction, threats, or hazards.<br>● The Company will develop, implement, and maintain an information security program designed to protect the confidentiality, integrity, and availability of the system and its information. | ● Logical access standards<br>● Physical access standards<br>● Employee provisioning and deprovisioning standards<br>● Security awareness training<br>● Access reviews<br>● Encryption standards<br>● Intrusion detection and prevention standards<br>● Risk and vulnerability management standards<br>● Configuration management<br>● Incident handling standards<br>● Change management standards<br>● Vendor management<br>● Regular security assessments<br>● Security policies and procedures |

# Signature Certificate

Reference number: BWRBS-I2GPB-SODPZ-3VSA5

| Signer | Timestamp | Signature |
|---|---|---|
| **Sothen**<br>Email: msothen@nationsafedrivers.com | | Michael Sothen |
| Sent: | 12 Nov 2024 18:52:43 UTC | |
| Viewed: | 13 Nov 2024 14:05:58 UTC | |
| Signed: | 13 Nov 2024 14:07:38 UTC | |
| **Recipient Verification:** | | |
| ✔Email verified | 13 Nov 2024 14:05:58 UTC | IP address: 209.160.213.154 |
| ✔Passcode | 13 Nov 2024 14:05:57 UTC | Location: Boca Raton, United States |
| **Amjad Khamis**<br>Email: amjad@aak-cpa.com | | Amjad Abu Khamis |
| Sent: | 12 Nov 2024 18:52:43 UTC | |
| Viewed: | 13 Nov 2024 15:57:33 UTC | |
| Signed: | 13 Nov 2024 15:58:15 UTC | |
| **Recipient Verification:** | | |
| ✔Email verified | 13 Nov 2024 15:57:33 UTC | |
| ✔Passcode | 13 Nov 2024 15:57:32 UTC | IP address: 20.115.217.120 |

Document completed by all parties on:

13 Nov 2024 15:58:15 UTC