PRIVACY POLICY AND STATEMENT

PURPOSE

This document outlines the privacy practices of National Software, Inc. (hereinafter referred to as "NSI") and provides transparency into how we collect, use, and protect personal data and includes two parts:

PRIVACY PROGRAM

Outlines the roles, responsibilities, and requirements of NSI to meet its privacy obligations. This includes the scope of applicable regulations and obligations related to NSI's data processing activities.

PRIVACY STATEMENT

A public-facing notice describing the purpose and use of personal data collected, as well as the privacy rights of individuals whose data is processed or stored by NSI. This statement is published on NSI's website and linked to systems and services that collect personal data.

REVISION HISTORY

Version	Updated by	Summary	Revision date
V1	Hariss Amin, Principal GRC Consultant	First version created	27-Oct-24

RESPONSIBILITIES

SENIOR LEADERSHIP TEAM

Accountable owner of this policy, including revision, updates, and communication. Ensuring NSI's privacy practices effectively meet the requirements and commitments of this policy.

Responsible for monitoring, enforcement and handling any breaches, or policy issues.

ALL EMPLOYEES

Responsible for reading, acknowledging, and supporting the requirements of this policy. Reporting any instances of non-compliance to Senior Leadership Team. Examples of non-compliance that employees should report include (data breaches, unauthorized data sharing, or non-adherence to this policy).

PRIVACY PROGRAM

JURISDICTIONAL APPLICABILITY AND SCOPE

The following privacy regulations, frameworks, and standards apply to NSI based on the jurisdictions and nature of data processing activities (Note: these regulations are non-exhaustive and subject to updates based on evolving laws):

Privacy Regulations	Purpose and Regulator	Key Obligations for NSI
California Consumer Privacy Act (CCPA)	Grants California residents enhanced privacy rights and consumer protections.	• **Right to Know:** Provide transparency about the categories and specific pieces of personal information collected, sold, or disclosed. • **Right to Opt-Out:** Ensure mechanisms for users to opt out of the sale of personal data. • **Right to Delete:** Enable California residents to request deletion of personal data, subject to legal exceptions.
Personal Information Protection and Electronic Documents Act (PIPEDA)	Governs data collection, use, and disclosure for commercial activities in Canada.	• Obtain informed consent for data collection and use. • Implement appropriate safeguards to protect personal data against unauthorized access. • Provide mechanisms for individuals to access and challenge the accuracy of their data.
Health Insurance Portability and Accountability Act (HIPAA)	Protects the privacy and security of individually identifiable health information (PHI).	• **Privacy Rule:** Ensure PHI is not disclosed without proper authorization, except as allowed under HIPAA. • **Security Rule:** Apply technical and organizational safeguards to protect electronic PHI (ePHI). • **Breach Notification Rule:** Notify affected individuals and the Department of Health and Human Services (HHS) of breaches involving PHI. • **Minimum Necessary Standard:** Limit access and use of PHI to the minimum required for the intended purpose.
IRS Guidelines	Establishes requirements for safeguarding taxpayer data and ensuring compliance with federal tax laws.	• Implement written information security plans (WISP) per IRS Publication 4557. • Encrypt taxpayer data during storage and transmission. • Ensure third-party service providers comply with IRS security guidelines.
Payment Card Industry Data Security Standard (PCI DSS)	Sets standards for securing credit card transactions and protecting cardholder data.	• Encrypt cardholder data during transmission. • Regularly test and monitor networks for vulnerabilities. • Implement access controls to restrict cardholder data access to authorized personnel.
Sarbanes-Oxley Act (SOX)	Mandates financial and operational controls to protect sensitive	• Ensure accurate and tamper-proof data logs for financial records. • Maintain audit trails for access to sensitive data.

	corporate and financial data.	• Conduct periodic internal audits of data management practices.

The following privacy requirements and obligations apply to NSI based on the personal data collection activities and scope above.

NOTICE AND TRANSPARENCY REQUIREMENTS

NSI is required to give notice to data subjects prior to processing of personal data (e.g., pop-ups, email notifications) and provide transparency around the purpose and use of their personal data.

References: **45 CFR § 164.520 - Notice of Privacy Practices for Protected Health Information**

LEGAL BASIS FOR PROCESSING

There must be a legal basis for the processing of personal data collected by NSI. That may include where consent is obtained, it's required to fulfil a contract, vital interests of the data subjects, for public or other legitimate interests.

References: 45 CFR § 164.506

PURPOSE LIMITATION

Personal data can only be collected for the specified and legitimate purposes, in line with NSI's Privacy Policy. The personal data cannot be further processed in a manner that is incompatible with those purposes.

References: 45 CFR § 164.502(b) - Minimum Necessary Requirement

DATA MINIMIZATION

Data minimization refers to NSI only collecting personal information that is directly relevant and necessary for the defined purposes of personal data collection. The personal data should only be retained for as long as is required to fulfil that purpose.

References: 45 CFR § 164.514(d) - Minimum Necessary Standard

SECURITY REQUIREMENTS

NSI is required to apply technical and organizational security measures that protect the personal data collected. That includes ensuring only authorized personnel have access to that personal data and taking reasonable steps (e.g., AES-256 encryption and periodic security audits conducted) to prevent data breaches.

References: 45 CFR Part 164, Subpart C - Security Standards for the Protection of Electronic Protected Health Information

RECORD KEEPING

NSI is required to retain records of processing activities, including details of the relationships with data controllers and sub-processors (as applicable), the purpose and categories of personal data processing, records of disclosures, and any other required records to document NSI's compliance with its privacy obligations under this policy.

References: 45 CFR § 164.316 - Documentation

DATA BREACH NOTIFICATION

Breaches of personal data will be reported to supervisory authorities (e.g., as required under applicable law, typically within 72-hours of becoming aware of the breach) and the data subject(s) whose data was part of the breach.

References: 45 CFR §§ 164.400-414 - Breach Notification Rule

DATA PROTECTION OFFICER

A Data Protection Officer is required to be appointed that is accountable for ensuring effective implementation, monitoring and reporting of NSI's privacy obligations in accordance with this privacy policy.

References: 45 CFR § 164.530(a) - Personnel Designations

PRIVACY STATEMENT

INTRODUCTION

When you use our services, we're collecting your personal data to support those services. Data privacy is important to us at NSI. This Privacy Policy details our use of personal data and your privacy rights and choices available to you.

HOW WE USE PERSONAL DATA

NSI collects personal data to:

- Personalize and improve user experience.
- Provide customer support and troubleshooting.
- Process and fulfill service requests

PERSONAL DATA WE MAY COLLECT

NSI may collect one or more of the following types of data as a requirement for using our services:

1. Name
2. Contact information
3. Home address
4. Date of birth
5. SSN
6. Credit card number
7. Taxpayer identification numbers
8. Business contact information
9. IP address
10. Cookie ID
11. Login and password
12. Usage data

WHEN WE SHARE YOUR PERSONAL DATA

NSI shares personal data with third parties only under lawful circumstances, including:

1. Compliance with legal or regulatory requirements.
2. Secure processing by sub-processors (as outlined below).

YOUR PRIVACY RIGHTS

You have the following rights:

1. **Right to be Informed:** Learn how and why your data is collected.
2. **Right to Access:** Request copies of your personal data and details about its use.
3. **Right to Rectify:** Correct inaccuracies in your personal data.
4. **Right to Erasure:** Request deletion of your personal data (subject to legal or operational requirements).
5. **Right to Restrict Processing:** Limit how your data is used.
6. **Right to Data Portability:** Transfer your data to another provider.
7. **Right to Opt-In for Sensitive Data:** Provide explicit consent for processing sensitive data.

These rights are subject to the clauses of the relevant privacy regulations, legal requirements, public interest, and where the above rights may conflict with your use of our services. For any privacy concerns or to request further details of your rights, please see the Privacy Requests and Contacts section below.

SUB-PROCESSORS AND LOCATIONS

To deliver our services, NSI engages third-party providers (sub-processors) who meet stringent security standards. See the complete list and their respective roles detailed below.

CLOUD SERVICE PROVIDERS

Webhost/Database: Hosts and processes application data.
Location: United States (primary hosting regions).

Google Workspace: Provides email, document management, and shared drive functionality and cloud functions.
Location: Global (specific locations depend on Google's data center allocations).

DATA BACKUP AND DISASTER RECOVERY SERVICES

CloudAlly: Backs up Google Workspace data, including email, Google Drive, and shared drives.
Location: United States and other regions as per their service architecture.

Supabase: Data processing & workflow records.
Location: United States and other regions as per their service architecture.

CUSTOMER SUPPORT PLATFORMS

Crexendo: VOIP phone provider used for customer communication.
Location: United States.

Direct Digital Division: Manages mail house operations for sending 1099 and ACA form data to employees of our customers.
Location: United States.

DocuSign: Provides digital signature solutions and acts as a backup for signed agreements.
Location: United States and other regions depending on their global operations.

ShareFile: Backup storage for application data and other critical files.
Location: United States.

PAYMENT PROCESSORS

Authorize.net: Processes payment transactions securely.
Location: United States.

Stripe: Processes payment transactions securely.
Location: United States and other global locations as per their operational model.

We remain committed to maintaining transparency about our sub-processors and their roles in processing customer data. If any changes occur to our list of sub-processors, we will update this Privacy Policy accordingly.

PRIVACY REQUESTS AND CONTACTS

For inquiries, complaints, or exercising your privacy rights, contact us:

Privacy Officer: Dave Woods, Security Risk Manager
Email: davew@1099fire.com
Mailing Address: PO Box 13001 Phoenix AZ 85070
Contact Page: https://www.1099fire.com/contact.htm

We attempt to respond to inquiries within 30-days.

End of Policy