NETCHANNELS MARKETING PERSONAL INFORMATION PROTECTION POLICY

1. Purpose

Netchannels Marketing, LLC a California corporation (”**Company**”) has adopted this “**Policy**” to govern the treatment of our customers’ and employees’ Personal Information. The loss of Personal Information can result in substantial harm to individuals, including embarrassment, inconvenience, and fraudulent use of the information. Protecting the confidentiality and integrity of Personal Information is a critical responsibility that must be taken seriously at all times. Compliance with this Policy is mandatory.

The purpose of the Policy is to:

- Define Personal Information.
- Establish general principles for protecting Personal Information.
- Assign accountability for protection of Personal Information.
- Ensure compliance requiring that covered entities implement and maintain reasonable security procedures and practices.

2. Scope

This Policy applies to all Company employees, agents, and representatives, including any contractor or third-party provider of services to the Company (”**Third-Party Service Provider**”) who have access to Personal Information the Company has collected or otherwise has in its possession. This Policy applies to all Personal Information collected, maintained, transmitted, stored, retained, or otherwise used by the Company regardless of the media on which that information is stored and whether relating to employees, customers, or any other person.

3. Definitions

”Personal Information” means information the Company has collected or otherwise maintains or has in its possession that identifies or can be used to identify or authenticate an individual, including, but not limited to:

- Names.
- Addresses.
- Telephone numbers.
- Email addresses.
- Employee identification numbers.
- Government-issued identification numbers.
- User passwords or PINs.
- User identification and account access credentials, passwords, PINs and security question answers.
- Financial account numbers.
- Geolocation data.
- Biometric, medical, health, or health insurance information.

”Data Subject” means the person about whom Personal Information is collected.

”Security Incident” means any act or omission that compromises the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards the Company or a Third-Party Service Provider has put in place to protect Personal Information. The loss of or unauthorized access to, disclosure, or acquisition of Personal Information is a security incident.

4. Using, Handling, and Retaining Personal Information

Notice and Collection. It is Company policy that whenever it collects Personal Information for any purpose, including for human resources or employment purposes, it must inform the Data Subject of how it will use, process, disclose, protect, and retain that Personal Information by presenting a privacy policy or privacy notice to the individual at the time the individual provides the Personal Information. You may only collect Personal Information in compliance with applicable Company policies, notices, and Data Subject consent, and the Personal Information collected must be limited to that which is reasonably necessary to accomplish the Company's legitimate business purposes or as necessary to comply with law.

Access, Use, and Sharing of Personal Information. You may only access Personal Information when the information relates to and is necessary to perform your job duties. You may not access Personal Information for any reason unrelated to your job duties. You may not use Personal Information in a way that is incompatible with the notice given to the Data Subject at the time the information was collected. If you are unsure about whether a specific use or disclosure is appropriate, you should consult with your supervisor. You may only share Personal Information with another Company employee, agent, or representative if the recipient has a job-related need to know the information. Personal Information may only be shared with a Third-Party Service Provider if it has a need to know the information for the purpose of providing the contracted services and if sharing the Personal Information complies with the privacy notice provided to the Data Subject.

Accuracy. You must collect, maintain, and use Personal Information that is accurate, complete, and relevant to the purposes for which it was collected.

Information Security Program. You are responsible for protecting Personal Information by understanding and complying with the Company's administrative, technical, and physical safeguards (the "**Information Security Program**") set forth below. Further, some of these safeguards include mandatory procedures that you must follow. If you do not understand any of the following safeguards, you must contact your direct supervisor for further instruction. More restrictive safeguards than those set forth herein may be implemented upon written notice to you, however, the Company's Information Security Program requires, at a minimum:

- **Administrative safeguards** including:
  - Designation of one or more employees to coordinate this Information Security Program to identify foreseeable internal and external risks, and assess whether existing safeguards adequately control the identified risks, currently CEO Laura Williams. You must report all Security Incidents to the designated employee as soon as is practicable;
  - Training employees in Information Security Program practices and procedures, with management oversight. You must ensure that you understand this Information Security Program and its limitations and ask for further instruction from your direct supervisor if you do not;
  - Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract, if you are required to select a service provider as part of your job duties; and
  - Adjusting the Information Security Program in light of business changes or new circumstances. You are encouraged to approach the designated employee should you perceive added risks due to business changes or new circumstances.

- **Technical Safeguards** through the use of software security systems covering the Company network. You are responsible for familiarizing yourself with and, to the extent required, implementing the Company's:
  - Secure user authentication protocols, including:
    - Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;
    - Restricting access to active users and active user accounts only and preventing terminated employees or contractors from accessing systems or records; and
    - Blocking a particular user identifier's access after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.
  - Secure access control measures, including:
    - Restricting access to records and files containing Personal Information to those with a need to know to perform their duties; and
    - Employing unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) that are reasonably designed to maintain security.
  - Encryption of all Personal Information traveling wirelessly or across public networks;
  - Encryption of all Personal Information stored on laptops or other portable or mobile devices;

  The Company will ensure that there is:

  - Reasonable monitoring of Company systems for preventing, detecting, and responding to unauthorized use of or access to Personal Information or other attacks or system failures;
  - Reasonably current firewall protection and software patches for systems that contain (or may provide access

to systems that contain) Personal Information; and
    - Reasonably current system security software (or a version that can still be supported with reasonably current patches and malicious software ("malware") definitions) that (1) includes malware protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

- **Physical safeguards** including:
    - Reasonable physical security measures to protect areas where Personal Information may be accessed. You are responsible to ensure that any Personal Information you handle, if stored physically, is stored in locked facilities, areas, or containers.
    - You must take reasonable measures to prevent, detect, and respond to intrusions or unauthorized access to Personal Information, including during or after data collection, transportation, or disposal; and

You must follow the security procedures set out in the Information Security Program at all times. You must exercise particular care in protecting Personal Information from loss, unauthorized access, and unauthorized disclosure.

***Retention and Disposal*.** You should keep Personal Information only for the amount of time it is needed to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. You must follow the applicable records retention schedules and policies and destroy any media containing Personal Information in accordance with the applicable records disposal policy.

5. Training Employees and Supervising Contractors

All Company personnel who have access to Personal Information must be educated and trained on this Policy and the treatment of Personal Information. In addition, whenever Personal Information is entrusted to a Third-Party Service Provider, proper management and supervision over the outside party's handling of that Personal Information must be ensured through appropriate contracts. Personnel with responsibility for supervising employees or managing Third-Party Service Provider relationships must be trained on supervision over those employees and Third-Party Service Providers.

6. Reporting a Security Incident

If you know or suspect that a Security Incident has occurred, do not attempt to investigate the matter yourself. Immediately contact your supervisor. You should preserve all evidence relating to the potential Security Incident.

7. Monitoring Compliance and Enforcement

Laura Williams is responsible for administering and overseeing implementation of this Policy and, as applicable, developing related operating procedures, processes, policies, notices, and guidelines. If you are concerned that any provision of this Policy, or any related policy, operating procedure, process, or guideline designed to protect Personal Information, has been or is being violated, please contact Laura Williams. The Company will conduct periodic reviews and audits to assess compliance with this Policy. Employees who violate this Policy and any related guidelines, operating procedures, or processes designed to protect Personal Information and implement this Policy may be subject to discipline.

8. Amendment and Revision

This Policy may be revised from time to time. This Policy was last revised on January 6th, 2025.

Acknowledgment of Receipt and Review

I, _____ (employee name), acknowledge that on _____ (date), I received a copy of Netchannels Marketing's Personal Information Protection Policy and that I read it, understood it, and agree to comply with it. I understand that Netchannels Marketing has the maximum discretion permitted by law to interpret, administer, change, modify, or delete this Policy at any time with or without notice. No statement or representation by a supervisor or manager or any other employee, whether oral or written, can supplement or modify this Policy. Changes can only be made if approved in writing by the CEO of Netchannels Marketing. I also understand that any delay or failure by Netchannels Marketing to enforce any work policy or rule will not constitute a waiver of Netchannels Marketing's right to do so in the future. I understand that neither this Policy nor any other communication by a management representative or any other employee, whether oral or written, is intended in any way to create a contract of employment. I understand that, unless I have a written employment agreement signed by an authorized [EMPLOYER NAME] representative, **I am employed at will and this Policy does not modify my at-will employment status.** If I have a written employment agreement signed by an authorized Netchannels Marketing representative and this Policy conflicts with the terms of my employment agreement, I understand that the terms of my employment agreement will control.

	_____ Signature _____ Printed Name _____ Date]