International Vitamin Corporation
Privacy Data Policy

1.0 Policy Statement

1.1 International Vitamin Corporation ("Company") has adopted this *Privacy Data Policy* governing the collection, use, and retention of Personal Information and the use of technology by employees. Information and technology are two of our most important assets, and it is everyone's responsibility at Company to preserve and protect our data, especially Personal Information. Compliance with this policy is of the utmost importance to the Company and is mandatory.

1.2 The purpose of the policy is to:

- Define Personal Information
- Establish minimum standards for handling Personal Information
- Assign accountability for protection of Personal Information at Company

1.3 This policy applies to all Personal Information collected, maintained, transmitted, stored, or otherwise used by Company in the conduct of its operations, regardless of the medium in which the information is stored. The audience for this policy includes all employees and contractors, as well as any third parties who have access to non-public Personal Information or other Company technology resources.

1.4 If there is any conflict between this policy and any other Company policy, the terms of this policy shall take precedence. Other policies may be applied in addition to this policy provided that the protections from the other policies are more restrictive or privacy-protective than the protections set forth in this policy.

2.0 What is Personal Information?

2.1 "Personal Information" is broadly defined as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, employee or household.

2.2 "Sensitive Personal Information" or "SPI" is a subcategory of Personal Information under this policy and includes (a) an individual's Social Security or other state identification number; (b) an individual's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (c) an individual's geolocation; (d) an individual's racial or ethnic origin, religious or philosophical beliefs, or union membership; (e) the contents of an individual's mail, email, or text messages, unless the business is the intended recipient of the communication; and (f) an individual's

genetic data. It also includes processing of biometric information for purposes of identifying an individual, Personal Information collected and analyzed concerning an individual's health, and Personal Information collected and analyzed concerning an individual's sex life or sexual orientation.

2.3 Notwithstanding the definition of SPI, nothing in this policy is intended to limit the Company's right to access, review and act upon any personal emails sent or received by any employee using the Company's email, servers or computer systems, or any information or data viewed or stored by any employee using the Company's servers or computer systems, which belong to the Company, so employees should have no reasonable expectation of privacy relating to any such use.

3.0 Protecting Personal Information

All Personal Information must be protected with the safeguards appropriate to its sensitivity. The following rules apply to everyone working for or on behalf of the Company:

3.1 Collect Personal Information Only as Authorized

- When you collect Personal Information, you must provide clear and conspicuous notice, at or before the time of collection, and obtain appropriate consent (if needed) for any intended uses. You must describe the choices available and explain the consequences of denying or withdrawing consent. The notice must explain the purpose, uses, retention, and disclosure of the information and identify the entities and activities covered by the notice.

- When collecting Personal Information, you must comply with all other Company policies that pertain to the collection.

3.2 Limit Use of/Access to Personal Information.

- Only access Personal Information when you need to know that information, that is, when your need for the information relates to your job duties. Do not access Personal Information for any non-job-related reason.

- Use must be compatible with notice given at time of collection. If Personal Information is to be used for new purposes not previously identified, in general new notice must be provided. If you are unsure about whether a specific use or disclosure is appropriate, you should confirm with your supervisor.

3.3 Share Personal Information Only as Authorized

- You are authorized to share Personal Information with another Company employee or contractor only if the recipient's need for the information relates to his or her job duties.

- You may disclose Personal Information to third parties only for the purposes identified in the notice at the time of collection and with appropriate consent (if needed), or as needed for routine business operations for which consent to the disclosure is reasonably inferred.

3.4 Minimize Collection of Personal Information

- You must limit the collection of Personal Information to what is needed to fulfill the purposes of the collection, as described in the notice.

3.5 Maintain Quality

- You must collect, maintain, and use Personal Information that is accurate, complete, and relevant. Departments shall establish (as necessary) and follow appropriate procedures for authenticating the identity of those submitting information, for assessing the accuracy and relevance of information over time, and for allowing individuals to submit updates and corrections.

3.6 Provide Access and Opportunity for Correction

- You must, as appropriate and within a reasonable timeframe and cost to the individual, provide individuals with access to their Personal Information in an understandable form for review, correction, and update.

3.7 Follow Records Retention and Disposal Policies

- You must treat Personal Information in accordance with the applicable records retention protocols. You may retain information extracted from a database or information system only as long as needed. When data is no longer needed, it will be disposed of securely.

3.8 Secure Personal Information

- The Company will, where appropriate, implement security tools such as encryption, secure development practices, multi-factor authentication, and change management practices.

- When you handle, process, transmit, or store Personal Information, you should limit the potential for unauthorized disclosure. To do this, protect against "shoulder surfing," eavesdropping, or overhearing by anyone without a need to know the Personal Information.

- If someone sends you Personal Information in an unprotected manner, you still must secure it once you receive it.

3.9 **Security Standards for Personal Information**

- Personal Information shall not be stored on devices or electronic folders that are not password-protected. For example, storage of Personal Information on external hard drives, thumb drives, or unsecured network drives is not appropriate.

4.0 Roles & Responsibilities

4.1 The Senior Human Resources leader, is responsible for implementing this *Privacy Data Policy* and shall coordinate with the Information Technology department to establish, maintain, update, and enforce a comprehensive information security program to protect Personal Information against loss, misuse, and unauthorized access, disclosure, alteration, and destruction. The Senior Human Resources leader will provide reporting annually to executive leadership.

4.2 Contracts and other agreements involving the collection, use, and retention of Personal Information must be reviewed for consistency with Company's privacy policies and procedures.

4.3 Management shall reasonably confirm that third parties from whom Personal Information is collected are reliable sources that collect information fairly and lawfully, and shall take remedial action in response to misuse of Personal Information by a third party to whom the Company has transferred such information.

4.4 Management shall annually review the assignment of personnel, budgets, and allocation of other resources to its privacy program.

4.5 Company shall ensure that employees responsible for protecting the privacy and security of Personal Information are qualified and trained for such responsibility through pre-hire background and reference checks. Sections 3.0 and 8.0 of this Policy set forth the requirements imposed on all employees to protect the confidentiality of Personal Information.

4.6 All employees shall receive periodic training on privacy protection and Company's privacy policies and procedures.

5.0 Risk Assessments, Monitoring & Enforcement

5.1 Company shall produce regular written risk assessments to evaluate risks and determine whether current safeguards are sufficient.

5.2 Company shall monitor and enforce compliance with privacy laws, internal policies and procedures, and its contractual commitments. It shall have mechanisms in place to address internal and external privacy-related inquiries, complaints, and disputes. Company shall have processes to document compliance, submit assessment reports to senior management, and develop remediation plans where appropriate. Staff and any

vendors with whom it shares Personal Information will be informed that compliance with privacy and security controls will be enforced. Such monitoring will include logging, and regular penetration testing and vulnerability assessments.

5.3 Failure to comply with Company's privacy policy is subject to discipline, up to and including termination.

6.0 Training

6.1 All employees shall be educated on the terms of this *Privacy Data Policy* at the time of their initial orientation and training, and each employee shall sign an acknowledgment regarding his or her knowledge of these policies.

6.2 In the event of changes to this *Privacy Data Policy*, all employees shall be notified.

7.0 Handling of Data Subject Requests

7.1 Consumers, employees, former employees and/or applicants may, from time to time, attempt to exercise certain rights available to data subjects under the EU's General Data Privacy Regulation ("GDPR"), the California Privacy Rights Act ("CPRA"), or some other similar statutes.

7.2 Under these statutes, if applicable, data subjects can request access to their data, deletion of their data, or to be removed from the Company contact list. Company cannot delete transactional data, but it can provide access to a consumer's data and it can delete non-transactional data.

7.3 Any Company employee that receives a data subject request of this nature should promptly notify the Senior Human Resources leader of the company.

8.0 Handling of Sensitive Personal Information

8.1 To the extent it is necessary to collect SPI – including, but not limited to biometric information collected from employees – the Company will treat it with the utmost care. The Company will limit its collection of SPI to only instances where absolutely necessary, and the Company will not use any such information to infer characteristics about consumers or employees.

8.2 Customers, employees, former employees and/or applicants may attempt to opt out of the use of SPI pursuant to applicable laws. Note, however, that such an opt out may not be permitted if the Company needs to utilize SPI for business purposes, such as when administering payroll. Any Company employee that receives a data subject request of this nature should promptly notify the Senior Human Resources leader.

9.0 Biometric Information

9.1 The Company collects fingerprints from certain employees, which it uses to identify employees, process payroll, and monitor time records.

9.2 The Company will use the reasonable standard of care within the industry when it collects and stores biometric data. Further, the Company's vendors have assured it that they will use the reasonable standard of care within the industry to protect any biometric data from disclosure.

9.3 Access to biometric information will be strictly limited to individuals who must access that data to carry out their job functions. The Company and its vendors will not sell, lease, trade, or otherwise profit from biometric data.

9.4 Any biometric data collected by the Company will be retained during the length of the employee's association with the Company and then the Company will take steps to permanently destroy any biometric data no more than one year from the earlier of: (i) the employee's last use of the Company's timekeeping system or timeclock, or (ii) the Company's use of the timekeeping system or timeclock which use the data has been permanently discontinued.

9.5 As a condition of their employment with the Company, certain employees will be required to sign a consent and release authorizing the Company, its vendors, and/or the licensor of the Company's time and attendance software to collect, store, and use their personal identity data.

10.0 Policy History/Revision Dates

Origination Date: 6/21/2024
Last Amended Date: 6/21/24