Statement and Purpose of Policy

ConnectAndSell, Inc. (the "Company") is committed to ensuring that all Personal Information (PI) handled by the Company will be processed according to legally compliant standards of data protection and data security.

1. **Definitions**. For the purpose of this Policy, following definitions of terms are in scope:
    I. Employee. Under practices of common law an Employee is an individual with "right of control" and for whom the Company pays employment taxes on their wages and reports their respective earnings to Employment Development Department (EDD).
    II. Contractor. All individuals who provide various services to the Company under contracts but has no "right of control" as defined under common law, irrespective of their seniority, tenures, or working hours, including all worldwide non-Employee directors, officers, consultants, casual or agency staff, trainees and interns, and advisors.
    III. Service Provider. Organizations that provides specific ongoing business services, such as payroll, benefits, insurance, etc. to the Company.
    IV. Customer. Organizations that either currently contractually subscribe to or had subscribed in the past or can potentially subscribe to Company's products to perform their business functions.
    V. Subject. Person to whom the information relates.
    VI. Third Party Data. Such PI data that the Company collects, stores, or processes that pertains to their Customer's customers or other contact data that are contractually sourced from their contact data providers.
    VII. Personal Information (the "PI"). Any information that can be used to identify an individual.
    VIII. Sensitive Personal Information (the "SPI"). Subset of the PI that may include social security numbers, government issued identification numbers, credit or debit card numbers, financial account information, driver's license number, information related to individual's health, race, ethnicity, religious or philosophical beliefs, trade union membership, political beliefs, sexual orientation, and criminal background.
    IX. Data Controller. Collects its own data and makes decisions about how the data is used.
    X. Data Processor. Receives data from others as-is only for using them for specific and agreed upon purposes

2. **Scope**. This policy and the rules contained in it apply to all Employees in United States and India, as well as all Contractors globally.
3. **Purpose**. This Policy is to help the Company achieve their data protection, privacy, and security aims by:
    - Notifying the Employees and Contractors of the types of PI that the Company may hold about them and what the Company will do with that information;
    - Ensuring that the Employees and Contractors understand the rules and the legal standards for handling PI – sensitive or otherwise, relating to the respective individuals; and
    - Clarifying the responsibilities and duties of the Employees and Contractors in respect of data protection and data security.
4. **Right to amend.** This is a statement of Policy only and does not form part of any employment or engagement contract. The Company may amend this Policy at any time, at their absolute discretion.

Data Protection and Data Security Responsibilities

5. **Owner**. The Company designates its Chief Technology Officer (CTO) to have the overall responsibility for ensuring that all PI is handled in compliance with the law and has appointed a senior engineer with day-to-day responsibility for implementing and monitoring all data processing and data security compliance. The CTO at his or her absolute discretion may choose to appoint additional members or appoint an appropriate committee to oversee the security & privacy compliance function.
6. **Teaming**. Maintaining appropriate standards of data protection and data security is a collective task shared between the Company, the Employees, the Contractors, and the Service Providers.
7. **Individual responsibility**. All Employees and Contractors have personal responsibility to ensure compliance with this Policy, to handle all PI consistently with the principles set out here and to ensure that measures are taken to protect the data security and privacy. Respective line managers have special responsibility for leading by example for monitoring and enforcing compliance.
8. **Penalty for breach.** Any breach of this Policy will be taken seriously and may result in disciplinary action.

Personal Information and Activities covered by the Policy

9. This policy covers the following PI scope:

    - that relates to a living individual who can be identified either from that information in isolation or by reading it together with other information Company possess;
    - that is stored electronically or on paper in a filing system;
    - that relates to Employees & Contractors (present, past or future) or to any other individual whose PI Company controls or processes;
    - that Company obtains, holds or stores, organizes, discloses or transfers, amends, retrieves, uses, handles, processes, transports or destroys.
    - OUT OF SCOPE: COMPANY DOES NOT COLLECT, STORE, OR PROCESS ANY CUSTOMER OR THIRD-PARTY SPI AND THUS WILL REMAIN OUT OF SCOPE FOR THE PURPOSE OF THIS POLICY.

Purpose of Collecting Personal Information

10. Company confirms that for the purposes of the data protection, the Company is a Data Controller of the Employee PI in connection with employment, and is a Data Processor for the Contractor, Customer, and Third-Party Data. This means that the Company determines the purposes for which and the manner in which the respective PI is handled.
11. Employees:
    I. Company or its Service Providers (on behalf of the Company) may collect certain PI, which Employees provide before or during the employment process and tenure with the Company.
    II. The types of PI that is collected, stored, and used about an Employee include records relating to:
        a. home address and contact details as well as contact details for next of kin;
        b. recruitment (including application form or cv, any references received and details of qualifications);
        c. pay records such as social security numbers or government issued identifications, immigration status, and any employment benefits such as health insurance (including details of any claims made);
        d. specific individual performance and any disciplinary matters, grievances, complaints or concerns.

III. Company may use information to carry out the business, to administer specific individual employment or engagement and to deal with any problems or concerns the Staff may have including:

a. **Staff Address Lists:** to obtain lists of home address and contact details, for contacting outside working hours, if needed.

c. **Monitoring IT systems:** to monitor use of business e-mails as well as use of internet, computer or other communications or IT resources within the Company's network.

d. **Disciplinary, grievance or legal matters:** in connection with any disciplinary, grievance, legal, regulatory or compliance matters or proceedings that may involve the Staff.

e. **Performance Reviews:** to carry out respective performance reviews.

Company will not use any of Employees PI for any purposes other than what is explicitly stated in this Policy.

V. The Employees will have access to their respective PI and may inform the Company and its Service Provider about any inaccuracy; if the Company agrees with the inaccuracy then the Company or its Service Provider will immediately correct it. If the Company does not agree with the reported inaccuracy then the Company will not update the information and notify the Employee accordingly.

VI. Employees consent that by providing their respective PI to the Company, Company may make use of that PI (including any SPI) in accordance with this Policy.

12. Contractors:

I. Company or its Service Providers may collect certain PI from its Contractors mostly for the purpose of contracts, payments, and taxes.

II. Company will protect such information and will not use or share it for any other purposes other than what is stated in this Policy with the exception of any regulatory, legal, or law enforcement needs and requirements.

13. Customers:

I. Company collects PI for certain persons (name, position, email, phone) for its Customer base to sell or market Company's products and services to. Company may run such campaign and communications either by themselves or appoint a Contractor to do so on its behalf and under its banner.

II. Company strictly honors opt-in policies and commits to not spam the individuals by providing an "unsubscribe" option to its marketing or sales campaigns.

III. Additionally, individuals may explicitly request to opt-out and Company will take appropriate steps to mark them as such for all future communications.

IV. As specified elsewhere in this Policy, Company will also remove their specific information altogether from its database pending receiving such request from individuals.

V. Company will never share Customer PI records with anyone for any purpose whatsoever other than what is specifically mentioned in this Policy.

14. Third Party Data:

I. Company processes Third Party Data either via an authorized engagement with its Customer or a contractual relationship with its contact data providers. Such processing will always be strictly within the authorized context and scope of the Customer engagement.

II. Company will not use Third Party Data for any other purposes than what it is intended for, specifically will not use that data for its own marketing and sales effort or share with anyone for any intent that is harmful to the Subject or causes stress.

III. Customer may request removal of certain set of Subject records to which Company is committed to comply expeditiously.

IV. Company will neither be responsible nor be held party to informing the Subject of the Third-party Data the purposes for which Company uses their PI; rather that responsibility will remain with the Customer and the respective contact data providers.

V. Outside of their own database, Company will only provide incremental or enriched PI Data to Customer via its relationship with its Third-Party Data providers when Customer bears the same responsibility of the lawful usage of that data and provide the same level of privacy and protections.

15. Company will take reasonable steps to ensure that PI is always kept secure, as described later in this policy and in general, the Company will not disclose any PI to others outside the Company, except:

I. for the needs to disclose Employee or Contractor PI:

- for the administration of employment and associated benefits, e.g. to the Service Providers of insurance and benefits; or
- to comply with any legal obligations or assist in a criminal investigation or to seek legal or professional advice in relation to employment issues, which may involve disclosure to lawyers, accountants or auditors and to legal and regulatory authorities, such as, IRS;

b. for the needs to disclose Customer or Third-Party Data:

- to other parties which provide certain services to the Company.

I. Such scenario will be strictly monitored and access provided purely on a need to know basis to a specific individual only for the duration that they need to render the service for.

II. Customers provide consent via contractual terms and conditions, that from time to time it may be necessary for the Company to allow its support, engineering, and development resources – employees or contractors, to be given access to the Third-Party Data for various analysis and / or monitoring.

III. In such scenario the respective Service Providers will contractually be bound to execute at least the same or more controls to protect and maintain privacy of such PI.

Data Protection Principles

16. Employees, Contractors, and Service Providers, whose work involves using any of the PI data must comply with this Policy and with the nine legal data protection principles which require that PI is:

a. **Processed fairly and lawfully.** Must always have a lawful basis to process PI. In most (but not all) cases, the Subject must have given consent, either implicitly or explicitly. The Subject must be told who controls the information, the purpose(s) for which the Company is processing the information and to whom it may be disclosed.

b. **Processed for limited purposes and in an appropriate way**. PI must not be collected for one purpose and then used for another. If Company wants to change the way PI will be used, Company must first tell the Subject.

**c. Adequate, relevant and not excessive for the purpose.**

d. **Accurate.** Regular checks must be made to correct or destroy inaccurate information.

e. **Not kept longer than necessary for the purpose.** Information must be destroyed or deleted when Company no longer needs it. CTO will provide necessary guidance on how long particular information should be kept.

f. **Processed in line with Subjects' rights.** Subjects have a right to request access to their PI, prevent their PI being used for direct-marketing (“opt-out”), request the correction of inaccurate data and to prevent their PI being used in a way likely to cause them or another person damage or distress.

g. **Removed in line with Subject’s rights.** Subjects have a right to request removal of their PI from Company’s database. Should such request

h. occur, Company must expeditiously and securely remove all respective PI and provide evidence of removal to the respective Subject.

i. **Secure.** See further information about data security below.

**j. Not transferred to people or organizations situated in countries without adequate protection.**

17. Some PI needs even more careful handling. This includes information, if collected or stored, about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life or about criminal offences. Strict conditions apply to processing this sensitive PI and the Subject must normally have given specific and express consent to each way in which the information is used.

    Data security

    Using appropriate data security measures, Company will take reasonable and appropriate measures to protect any PI from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

18. Maintaining data security means making sure that:

    a. Staff, only who are authorized to use the information can access it;

    b. Information is accurate and suitable for the purpose for which it is processed; and

    c. Authorized Staff can access information if they need it for authorized purposes which precludes any copying of the PI outside of the system they are captured, stored, and processed. PI therefore should never be stored on any Staff computers or devices.

19. By law, Company must use procedures and technology to secure PI throughout the period that Company hold or control it, from obtaining to destroying the information.

20. PI must not be transferred to any person or provider to process (e.g., while performing services for the Company on or its behalf), unless that person or provider has either agreed to comply with the Company's data security procedures or the Company is satisfied that other adequate measures exist.

21. Security procedures include:

    a. **Physically securing information.** Any desk or cupboard containing confidential information must be kept locked. Computers should be locked with a password or shut down when they are left unattended and discretion should be used when viewing PI on a monitor to ensure that it is not visible to others.

b. **Controlling access to premises.** Premises are access controlled physically through badge and keys. Staff should report to security if they see any person they do not recognize in an entry-controlled area.

22. Telephone Precautions. Particular care must be taken by Staff who deal with telephone enquiries to avoid inappropriate disclosures. In particular:
    a. the identity of any telephone caller must be verified before any PI is disclosed;
    b. if the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing;
    c. do not allow callers to bully into disclosing information. In case of any problems or uncertainty, contact the CTO.
23. **Methods of disposal.** Copies of PI, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

Subject access requests

24. By law, any Subject (including Staff) may make a formal request for information that Company holds about them, provided that certain conditions are met. The request must be made in writing. In some circumstances it may not be possible to release documents containing information about the Subject to them e.g., if it contains PI about other individuals but the in such cases, the respective information about the Subject can be released or communicated without sharing the full document.
25. Any member of staff who receives a written request should forward it to the CTO immediately for approval, without which information should not be released.

Who can you contact for any questions?

26. The Company has an established office and channel for all related communications and questions around data security, privacy, and protection. Company encourages all inquiries and communications be in writing via emails to system@connectandsell.com