# **EMPLOYEE DATA PRIVACY POLICY**

**Scope and Application**

This Employee Data Privacy Policy outlines the principles **Sample Land Trust** (“**SLT**”) seeks to observe regarding the collection, use, disclosure, security, and disposal of personal information for its current and former employees and applicants.

**Employee Personally Identifiable Information**

**SLT** generally will collect personally identifiable information (“PII”) from employees, and create and maintain records about employees that contain employee PII, only for legitimate company purposes and only to the extent necessary to achieve those purposes. PII includes first name or initial and last name in combination with any of the following categories of information: Social Security Number, passport numbers, state identification cards, alien registration numbers, employee identification number, driver’s license number, date of birth, maiden name, mother’s maiden name, credit card, debit card or financial account information, health insurance identification number, military identification, results of background checks, payroll and salary information, medical information, accommodation requests and related information, and/or digital or other electronic signature files.

**Collection and Use of Employee PII**

**SLT** typically will collect, create, and maintain employee PII only in connection with the employment relationship. **SLT** may collect, create, use, or maintain employee PII needed for payroll administration, to provide health insurance and other benefits, to evaluate leave requests made by employees, to determine fitness for duty, as part of the reasonable accommodation process, during an investigation of misconduct related to work, or for various other purposes.

The records and databases that contain employee PII are the property of **SLT**, and access to the information they contain is restricted. **SLT** employees may not access, use, or disclose employee PII unless authorized to do so and then only for legitimate business purposes. The executive director, or their delegate, is responsible for establishing appropriate authorization. Employees with authorized access are required to limit their use and disclosure of employee PII to those legitimate purposes for which access was granted.

**Safeguarding Employee PII**

**SLT** is committed to safeguarding the confidentiality, integrity, and availability of employee PII through the use of reasonable and appropriate physical, administrative, and technical safeguards. Employees authorized to access employee PII should consider the following guidelines when handling employee PII:

* Employees authorized to access employee PII should not leave documents, including electronic documents, containing employee PII unattended unless secured in a restricted area or locked in a file cabinet, desk drawer, or office. Electronic documents should be saved and closed in a manner consistent with this policy.
* Documents containing employee PII generally should not be transmitted over the Internet unless encrypted.
* Envelopes containing employee PII, whether sent by company mail or other means, should be sealed.
* Employee PII should be removed from the electronic resources of employees who leave **SLT** before those resources are re-issued to another employee unless the successor employee has the same authority to access employee PII.

**Additional Safeguards For Social Security Numbers**

Employee Social Security Numbers (“SSNs”) and documents containing Employee SSNs should receive the following additional protections:

* SSNs generally should not be printed on paper documents that are mailed unless the document, by law, is required to include an SSN (such as a W-2 Form) or in certain other limited circumstances;
* SSNs should not be transmitted over the internet unless encrypted.

**Disposal of Employee PII**

Disposal of documents containing employee PII should be accomplished in a manner intended to prevent unauthorized access to such employee PII. For example, paper documents containing employee PII should be shredded. Employee PII stored on electronic media should be subject to processes, before disposal or reassignment, that render the employee PII irretrievable.

**Disclosure and Use of Employee PII by Third Parties**

**SLT** generally will disclose an employee’s PII to third parties who are not acting as service providers for **SLT** only with an employee’s consent, when required by law or in connection with a legal or regulatory proceeding or process, or when disclosure is otherwise necessary or advisable. **SLT** may disclose employee PII to its third-party service providers, including but not limited to benefit, payroll and workers’ compensation administrators.

**Violations of the Employee Data Privacy Policy**

**SLT** is committed to ensuring that employee PII is handled in accordance with this Employee Data Privacy Policy. Anyone who is aware of a suspected or perceived violation of this policy should immediately contact the executive director. Employees who violate this policy will be subject to discipline, up to and including termination.

**Legal Effect and Changes to the Policy**

This policy is not, nor is it intended to be, a contract, nor does it otherwise create any legal rights or obligations. **SLT**, in its sole discretion, may amend, interpret, modify or withdraw any portion of this and related practices with or without notice. Any change in this policy will apply to employee PII collected before the change went into effect.