

SRI LANKA CLIMATE FUND

SAMPATHPAYA, NO.82,
RAJAMALWATTA ROAD
BATTARAMULLA

DATA PROTECTION POLICY

This document details data protection policy maintained by Sri Lanka Climate Fund. It must not be reproduced in whole or in part or otherwise disclosed without prior written consent from relevant authority of the company.

Doc No	: SLCF-GHG-PLC-002
Issue No.	: 02
Date of Issue	: 10.01.2020
Rev. No.	: 01
Date of Revision	: 21.06.2021

SRI LANKA CLIMATE FUND	
Title: Data Protection Policy	Doc. No: SLCF-GHG-PLC-002
Issue No.: 02	Date of Issue: 10.01.2020
Rev. No: 01	Date of Rev.: 21.06.2021
Prepared by: Quality Manager	Reviewed and approved by: CEO

1. Introduction

Data Protection Policy of Sri Lanka Climate Fund (Pvt.) Ltd. indicates that we are dedicated to and responsible for safeguarding the data and information of our clients, stakeholders, employees and other interested parties with absolute caution and confidentiality. This policy details data protection requirements of GHG Verification Management System which is developed, implemented and maintained for the verification activities of organization and product level GHG statements. Policy elements including in this document provides detailed and explicit guidance on how we collect, store, handle and secure our data fairly, transparently and with confidentiality.

This policy ensures that SLCF follows good practices to protect the data gathered from its clients, employees, and stakeholders. The rules outlined in this document apply regardless of whether the data is stored electronically, on paper or on any other storage device.

2. Scope

Policy elements described in this document are applicable to data receiving, communication and handling processes associated with the verification activities of ISO 14064-1: 2018 and ISO 14067: 2018.

3. Roles and Responsibilities

Everyone who works for or with SLCF is responsible for ensuring that the collection, storage, handling, and protection of data is being done appropriately. The contact person responsible for managing the Data Protection Process is:

Person: Quality Manager
Email: info@climatefund.lk
Phone: 011 2053065

4. Policy Elements

4.1. General data management rules

As a key part of our verification activities, we gather and process any information or data that makes an individual or organization identifiable such as name, physical address, email address, photographs, etc.

This information is collected only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply to our company.

Our data will:

- Be precise and consistently updated;
- Be collected legitimately and with a clearly stated purpose;
- Be processed by the company in line with its legal and ethical binds;
- Have protection measure that protects it from any unauthorized or illegal access internal occurring by or external parties.

Our data will NOT:

SRI LANKA CLIMATE FUND	
Title: Data Protection Policy	Doc. No: SLCF-GHG-PLC-002
Issue No.: 02	Date of Issue: 10.01.2020
Rev. No: 01	Date of Rev.: 21.06.2021
Prepared by: Quality Manager	Reviewed and approved by: CEO

- Be communicated informally;
- Exceed the specified amount of time stored;
- Be transferred to organizations, stakeholders that do not acquire proper data protection policies;
- Be spread to any party unless approved by the data's owner (except for the legitimate requests demanded from law enforcement authorities).

4.2. General guidelines for employees

- Access to data covered by this policy is restricted only to those who need it for their work;
- Data is not to be shared informally. When access to confidential information is required, employees request it from their managers or chief executive officer;
- We provide formal training sessions to all employees to help them understand their responsibilities when handling data;
- Employees keep all data secure, by taking sensible precautions and following the Data Storage guidelines specified below;
- In particular, strong passwords are used and never shared;
- Personal data is not disclosed to unauthorized people, within the company or externally;
- Employees request help from their managers or the chief executive officer when they are unsure about any aspect of data protection.

4.3. Data Gathering / Receiving

In the current business scope, data gathering and receiving is one of most prioritized process of company. When employees engaged in data gathering and receiving following conditions are applicable.

- Data from a client or stakeholder can be collected and received via a confidential and secure communication channels.
- Data receiving purpose and its application should be informed to both client and internal responsible person of the company.
- If admitted, requested data is unreliable, data receiving and gathering can be suspended or rejected.

4.4. Data Storage

These rules describe how and where data are safely stored. When data is stored on paper, it is kept in a secure place accessed only by authorized personnel.

These guidelines also apply to data that is usually stored electronically but has been printed out for certain reasons:

- The paper or files are kept in a locked drawer or filing cabinet;
- Employees make sure paper and printouts are not left unattended;
- Data printouts are securely shredded and disposed when no longer needed.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious internal or external threats.

- Data should be protected by strong passwords that are updated regularly and never shared among employees;

SRI LANKA CLIMATE FUND	
Title: Data Protection Policy	Doc. No: SLCF-GHG-PLC-002
Issue No.: 02	Date of Issue: 10.01.2020
Rev. No: 01	Date of Rev.: 21.06.2021
Prepared by: Quality Manager	Reviewed and approved by: CEO

- If data is stored on removable media (like a CD or DVD, External HDD, etc.), these should be kept locked away securely when not being used;
- SLCF Network of computers is restricted from using or transferring any data via a CD, DVD, USB, and External HDD, unless authorized for specific personnel with additional privileges;
- Data should only be stored on designated computers at SLCF premises, and should only be uploaded on to approved cloud computing services;
- computers containing data are protected by the monitoring system and the firewall system;
- All data entering into SLCF systems and website are stored as associated with a specific user account to and measures to prevent privilege escalation are always in place;
- All data entering into the database of the SLCF website are protected with strict security system.

4.5. Data usage

- All data collected by SLCF is strictly for SLCF-related services required to ensure a complete response/ service is being provided by SLCF. No other non-SLCF related service will be offered from the data collected;
- When working with personal data, employees ensure their computer screens are always locked when left unattended;
- Data is encrypted before being transferred electronically;
- Employees do not save copies of personal data into their own computers. The access and update of a copy is always made at the central copy of the data

4.6. Data accuracy and actions

To exercise data protection, SLCF takes reasonable steps and is committed to:

- Restrict and monitor access to sensitive data, and keep it in as few places as possible;
- Establish effective data collection procedures;
- Provide employees with online privacy and security measures training;
- Build secure network to protect online data from cyber-attacks;
- Establish clear procedures for reporting privacy breaches or data misuse;
- Include contract clauses or communicate statements on how we handle data;
- Update the data continuously and as mistakes are discovered;
- Install tracking logs to monitor employee's activities ensuring data is not being misused;
- Install firewall and protection software that prevents employees to share and distribute data from SLCF devices externally, by detecting when a large amount of data is being transferred either through email, or via external drives;
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.).

4.7. Obligation by outsourced entities

In the instance where internal staff does not have adequate competency and capacity to perform due activity pertaining to the GHG verification management system, the management of SLCF is

SRI LANKA CLIMATE FUND	
Title: Data Protection Policy	Doc. No: SLCF-GHG-PLC-002
Issue No.: 02	Date of Issue: 10.01.2020
Rev. No: 01	Date of Rev.: 21.06.2021
Prepared by: Quality Manager	Reviewed and approved by: CEO

authorised to outsource qualified personnel for the said respective activities. Prior to the undertaking of assignment, the both parties are entered into a formal consultancy service agreement/ contract where terms are set to safeguard confidentiality in handling and application of data as follows,

- Data received from SLCF shall be used only for the agreed assignment.
- Data shall be erased or destroyed at the end of the task/assignment
- If assisted or consulted by external entity, necessary confidentiality obligation shall be sought from the said entity.

4.8. Subject access requests

All individuals and organizations who are the subject of personal and other data held by SLCF are entitled to:

- Ask what information SLCF holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

a. Data Modification

Our clients can contact us requesting data modification and/or correction by sending an email to info@climatefund.lk or writing to SLCF Registered Office Address; P.O. Box No 18, 'Sampathpaya', No.82, Rajamalwatta Road, Battaramulla. SLCF will verify the identity of anyone making a data subject access request before modifying or correcting any information

b. Data Erasure

Our clients can contact us requesting data erasure via email at info@climatefund.lk or writing to SLCF Registered Office Address; P.O. Box No 18, 'Sampathpaya', No.82, Rajamalwatta Road, Battaramulla. In addition, data subject will be provided with all necessary information before proceeding with erasure.

Before proceeding with the erasure, the data subject will read the statement of our quality manager, explaining the outcome of the data being deleted. Erasure of data can be requested at any time.

4.9. Disclosing Data

In certain circumstances, when required, SLCF can disclose data to law enforcement agencies without the consent of the data subject. However, the data controller will ensure the request is legitimate, seeking assistance from the Board and from the company's legal advisers where necessary.

SRI LANKA CLIMATE FUND	
Title: Data Protection Policy	Doc. No: SLCF-GHG-PLC-002
Issue No.: 02	Date of Issue: 10.01.2020
Rev. No: 01	Date of Rev.: 21.06.2021
Prepared by: Quality Manager	Reviewed and approved by: CEO

5. Reference

SLCF-GHG -PLC-002 -01: Confidentiality Statement