Data GovernancePolicy

November 2020

Contents

Review History

DateofthisReview:26/11/2020	Dateofnextreview:26/11/2021
Date of Revision 01: 24/11/2022	Dateofnextreview:26/11/2023

Document Location

Website – Resources> Policies & Guidelines

Review Result

Reviewed By:	Debasish Dutta
Issued Date:	26/11/2020
Approved By:	Rajesh Bhuyan
Revision No.:	0
Reviewed By:	Debasish Dutta
Issued Date:	24/11/2022
Approved By:	Rajesh Bhuyan
Revision No.:	01

This Policy was agreed by the trustea Council on 29/01/2021. It shall be reviewed and, as necessary, amended by the Institute annually. All amendments shall be recorded on the revision history section above.

1. OVERVIEW

The trustea Sustainable Tea Foundation is responsible for the processing of a significant volume of information across each of projects, general administration, facility management and audit / certification. It is vital that everyone is aware of their responsibilities in relation to data protection as follows:

- Itistheresponsibilityofeachteam membersandFunctiontoensurethisinformationisprocessedina manner compliant with the relevant data protection legislation andguidance.
- Trustea has an appointed IT Manager ('ITM') who is available to all projects and activities to provide guidance and advice pertaining to thisrequirement.
- All Staff must appropriately protect and handle information in accordancewiththeinformation's classification.
- Confidential Information requires the greatest protection level (e.g. certification data).

This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

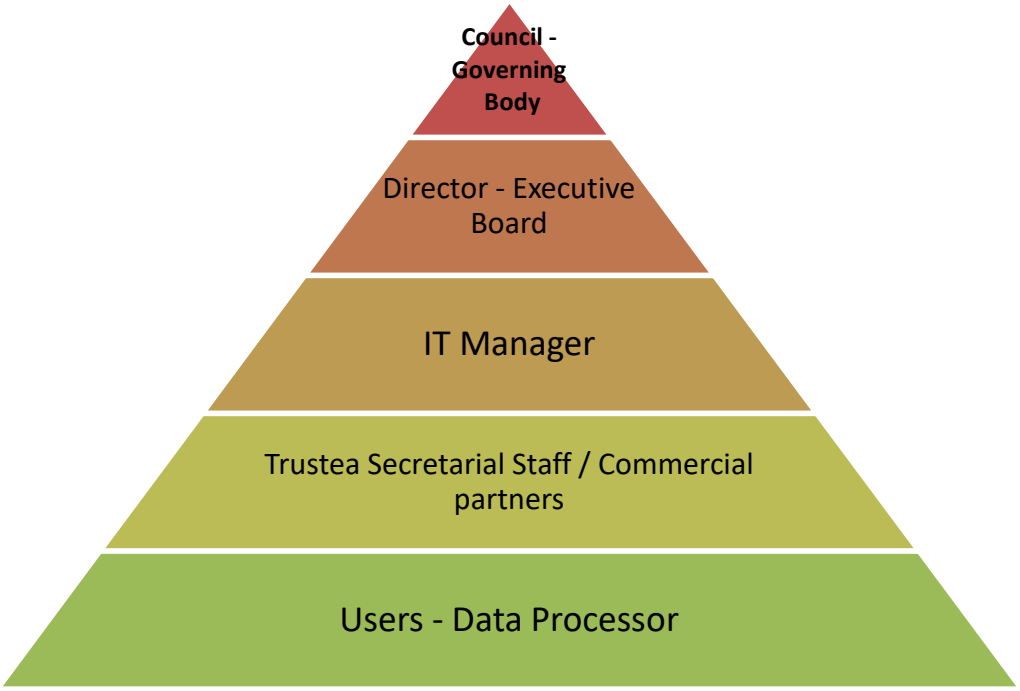
2. PURPOSE

To provide direction on the classification, ownership and retention of data and information for trustea as well as clarifying accountability for data and information. Data and information as pertaining to this policy includes electronic and non-electronic data.

trustea is reliant upon the confidentiality, integrity, and availability of its data and information to successfully conduct its operations, meet stakeholders and team members expectations, and provide services.

Therefore, all staff, certified entities, audit bodies, and partners of trustea have a responsibility to protect organization data and information from unauthorized generation, access, modification, disclosure, transmission or destruction and are expected to be familiar with and comply with this policy.

3. ROLES ANDRESPONSIBLITIES



The following roles and responsibilities apply in relation to this Policy:

Governing Body	To review and approve the policy on a periodic basis
Executive Board	The Executive Board (EB) is responsible for the internal controls of trustea an element of which is the retention of records used in the decision-making process for key decisions in order to demonstrate best practice and the assessment of risk. The EB is responsible for: • Reviewing and approving this Policy and any updates to itas recommended by the trustea Secretariat. • Ensuring ongoing compliance with the Data Policy in theirrespectiveareas of responsibility. • Ensuring oversight of data protection issues either throughtheirown work or a Data Protection Oversight Committee or another governance arrangement.
IT Manager	• To lead the data protection compliance and riskmanagement function, with responsibility for advising how to comply with applicable privacy legislation and regulations. • To advise on all aspects of data protection and privacyobligations. • To monitor and review all aspects of compliance withdata protection and privacyobligations. • To act as a representative of data subjects in relation tothe • processing of their personal data. • To report directly on data protection risk and complianceto executive management.
Staff/authorized users	• To adhere to policy statements in thisdocument. To report suspected breaches of policy to Director trustea and/or IT Manager.
Data Processor	• Management and staff within the trustea who take responsibility for processing, storing and/or archiving Institute data. Data processors take responsibility to apply the relevant information handling controls required per the classification of data set out in section 5 below.

4. SCOPE

This Data Governance Policy relates to all trustea's data including but not limited to:

- Trustea Certified EntitiesData
- Trustea StaffData
- Trustea FinancialData
- Trustea CommercialData
- Trustea IntellectualProperty
- Assurance system data
- Trustea's digital application data
- Trustea's data value chain (Appendix D)

trustea is committed to ensuring that all trustea data is clearly identified and an inventory of all important data is drawn up and maintained. The data inventory includes data held on all IT resources and application types including Microsoft (MS) Excel spread sheets, MS Access databases and other such end user application. Appendix B provides a template for the maintenance of a data inventory.

This policy applies to:

- Anypersonwhoisemployedbytrusteawhoreceives,handlesorprocessesdatainthecourseof theiremployment.
- Any external stakeholders of trustea who receive, handle or process data in the course of their assignment/activitiesforadministrative, research, certification, facilitation or any other purpose.
- Third-partycompanies(dataprocessors)thatreceive,handle,orprocessdataonbehalfof trustea.
- This applies whether you are working in the trustea, traveling or workingremotely.
- Authorised users of trustea's digital applications

5. POLICY

This policy should not be viewed in isolation. Rather, it should be considered as part of the trustea's suite of Data Protection policies and procedures (see Appendix A); in particular please refer to Data Handling & Clean Desk Policy for further information on the minimum requirements for handling data and maintaining a "clean desk".

5.1 Information Governance

5.1.1 Data Ownership

All information and assets associated with information processing facilities (applications) should be owned by a designated part of the organization. Therefore, data ownership to key sets of information and data (and associated applications) must be formally assigned.

Ownership of data resides with trustea and implies authority as well as responsibility and control. The control of information includes not just the ability to access, create, modify, package, and derive benefit from, but also the right to assign these access privileges toothers.

Inthecontextoftrusteadataownershipresponsibilitywillbeformallyassignedforthefollowing functional domains/process but is not limited to thesefunctions:

- Trustea Code and training materials
- Entity Certification and audit data
- Entity supply chain and traceability data
- Financialprocesses
- ResourcePlanning.

Data ownership responsibilities include:

- Approval of useraccess
- Approval of userroles/profiles/classes
- Review of access including application data held in network directorylocations
- Dataclassification
- Data retention rules anddefinition
- Master data changesauthorization
- Ensuring the availability ofinformation
- Data restorationtesting
- Service level management andmonitoring.

5.1.2 Data Classification

The purpose of information classification is to ensure that information/data receives an appropriate level of protection.

Following on from this, trustea classifies its data based on the level of impact that would be caused by inappropriate access and/or data loss. There are three classifications as follows:

Impact Level	*Types of Classification*
High	Confidential data (+ Strictly Confidential Data)
Medium	Internal Use Only data
Low	Public data

Classification of data is independent of its format. The following table provides an indication of how classifications get assigned by considering the impact of various risks:

Risk	**The impact is considered from four main perspectives- legal, reputational, financial, and operational**		
Inappropriate access causing a breach of confidentiality/data protection rules	**Serious**	**Moderate**	**Minor**
Inappropriateaccess resulting in unauthorized amendments	**Serious**	**Moderate**	**Minor**
Data loss	**Serious**	**Moderate**	**Minor**
Unauthorizeddisclosure	**Serious**	**Moderate**	**Minor**

Resulting Data Classification	**Confidential Data (+ Strictly Confidential Data)**	**Internal Use Only**	**Public Data**

Data Classification examples	• Finance Datarelating to trustea operation and personnel • HRData • Trustea audit and certification data • Supply chain and production data of certified entities	• Intranet / Extranet data • Internaltelephone books and directories • Financial Budgets	• PublicWebsites • CampusMaps • StaffDirectory
	Strictly Confidential • *Special Categories of Personal Data.*		

Confidential Data

Confidential data is information or data protected by statutes, regulations, Institute policies or contractual obligations. Personal data is considered to be **confidential** *or* **strictly confidential** data (see distinction above). Prior to the distribution or transmission of confidential data, it is required that reference is made to relevant legislation, (which at this time is the General Data Protection Legislation or GDPR) to ensure such distribution or transmission is not in breach of same. Confidential data should only be disclosed to authorized individuals on a need-to-know basis and in accordance with the relevant legislation. By way of illustration only, some examples of confidential
(C) and strictly confidential **(SC)** data include:

- Trustea operation data**(SC)**
- Certified units record and their production and supply chain data**(C)** or**(SC)**
- Verified growers' data**(C)**
- Personnel and payroll records**(C)**
- Bank account numbers and other personal financial information**(C)**
- Financial budgets [Commercially Sensitive –**(C)**].

Confidential data, when stored in an electronic format, must be protected with strong passwords and stored on servers that have appropriate access control measures in order to protect against the loss, theft, unauthorized access and unauthorized disclosure.

Confidential data must not be disclosed to parties without explicit management authorization. Confidential data must only be used for the purpose for which it was originally gathered. If, for legitimate teaching, learning and/or research activities confidential data is used for a purpose other than that of which it was originally gathered the data must be anonymized.

Internal Use-Only Data

Internal-only data is confidential information that must be protected due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. Internal use data is information that is restricted to members of the trustea community who have a legitimate purpose for accessing such data.

By way of illustration, only, some examples of official use data include:

- Intranet / Extranetdata.
- Internal telephone books anddirectories.
- Contact, Email address etc

Internal Use only data must be protected to prevent the loss, theft, unauthorized access and/orunauthorized disclosure.

Public Data

Public data is information that may be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data can be made available to all members of the trustea's community and to all individuals and entities external to the Trustea's community.

By way of illustration, only, some examples of public data include:

- Publicly-posted content on all external-facing websites
- Publicly-posted press release
- Publicly-posted schedules ofclasses
- Publicly-posed interactive guidelines, newsletters, newspapers andmagazines.

5.1.3 Data Review: The designated reviewer of the data as per the data value chain is the primary function that uses the data for managing the operation, analysis, reporting and improvement plans. The reviewer will ensure adequate due diligence and verification of the integrity of the data. In case there is any discrepancy the same will be discussed with the collator of the data to ensure accuracy.

The following steps will be used to ensure accurate and quality data:

Step 1 - Data producer enters the data

Step 2 – Data is reviewed by the data reviewer

Step 3 – If the data reviewer is satisfied the data retained

Step 4 – If the data reviewer finds inconsistency or inaccuracy, he/she requests the producer to look into the issue and restart the process from step one after taking corrective action

Step 5 – If any stakeholder who is a consumer of the analysis based on the data finds any issue with the data then step number 4 is to be initiated.

Step 6 – Any actionlinked to an external malicious attack may lead to the corruption of data. Once this is cleared by IT then actions will have to be initiated on the steps above after review by the data reviewer.

5.1.4 Retention of Data

It is the responsibility of data owners to clearly indicate the maximum period of time information/data should be retained by the Institute.

Please refer to Data Retention Policy for information on retention periods.

6. POLICYCOMPLIANCE

6.1 Compliance

Breaches of this policy may result in data breaches under data protection legislation, reputational damage to trustea, and an infringement of the rights of employees or other relevant third parties.

6.2 ComplianceExceptions

Any exception to the policy shall be reported to the IT Manager in advance at dutta@trustea.org

6.3 Non-Compliance

Failuretocomplywiththispolicymayleadtodisciplinaryaction,beingtakeninaccordancewiththe trustea's disciplinary procedures. Failure of a third-party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legalaction.

Non-compliance shall be reported to the IT Manager in advance at dutta@trustea.org

7. Communication and training:

The primary accountability for communication and training of the requirement related to data governance lies with the IT Manager. There are three types of communication that will be followed to ensure successful compliance to the data governance policy

7.1 Onboarding – when a new employee is onboarded the IT manager will ensure training, communication and confirmation of understanding for the following –

a. Nondisclosure agreement
b. Data security policy
c. Data Privacy Policy
d. Data Governance Policy
e. ISMS Policy

7.2 **Ongoing –** during the ongoing operation the IT Manager will ensure that any changes or new addition that impacts the management and handling of data are communicated to the employees and other concerned users of the company application.

7.3 **Emergency Communication -**In case of any data-related emergency or incident the IT manager will communicate all concerns as per the requirements of the situation.

APPENDIX A: DATA / BACKUP REGISTER

Note: Please refer to Data Retention Policy for further information on retention periods. Excel copy available from the ITM via email dutta@trustea.org

Program	Tool	Sub Tools	Activity	Primary User	Access	Critical	Backup		Alternate PPL/Note
							India (1)	India (2)	
trustea	tracetea - traceability solution	tracetea (mobile app)	STG level - Farm Diary, Plucking Data management, supply to factory, Culivation Support	Farmer, Lead farmer, Aggregator	Public User, trustea_admin	Moderate	IT Manager		At Playstore level only the application is stored. Data is with aCloud server. Backup Procedure - Scheduled / Autobackup, Storage –NICSI DC
			Aggregator Level - Collection and Supply of leaf from Grower and to factory respectively	Lead farmer, Aggregator	Public User, trustea_admin	High	IT Manager		
			Factory level - weighment, leaf receipt	Factory User	Public User, trustea_admin	High	IT Manager		
		tracetea (web app)	Factory Level - Production, Invoice and Warehouse, Salepool management	Factory User	Public User, trustea_admin	High	IT Manager		3 Tier application and database are in Cloud server, Backup Procedure - Scheduled / Autobackup, Storage - NICSI DC
			Tea Estate Level - Leaf Collection from the garden, collection in the factory, production, invoice, warehouse and sale pool management	Estate User	Public User, trustea_admin	High	IT Manager		
			Advisory/Expert Level - Tracking queries from field, Advisory Help to STG / Estate	Advisor	Public User, trustea_admin	Low	IT Manager	Director	
			Buyer / Consignee Level - Tracking Invoice, Backward and Forward Traceability	1. Factory User 2. On permission – Tea Buyer	Public User, trustea_admin	High	IT Manager		
			trustea Admin - All level user creation, roll management, Master data management, Advisory help matter monitoring, MIS / Report generation, QR card generation	trustea	trustea_admin	High	IT Manager	Director	
		tracetea (SMS Utility)	Message propagation among grower, aggregator, factory, estate and advisor regarding supply chain information	trustea (Auto-generated)	trustea_admin	High	IT Manager	Director	Managed service from Sendgrid, Backup Frequency - Alternation day(s)

Program	Tool	Sub Tools	Activity	Primary User	Access	Critical	Backup		Alternate PPL/Note
							India (1)	India (2)	
	trustea - Web portal		Changes on trustea website	Communication Manager / IT Manager	Sub System Admin, Admin	High	IT Manager	Communication Manager	Managed backup service. Backup Frequency - Weekly (Automatic)
			trustea website back-end management	IT Manager	Admin	High	IT Manager		
	Trustea CMS		Certification Body Level - Audior creation / management, Auditor monitoring, Audit Plan management, Entity and STG data management, Verification Certificate [VC] management	Certification Body	Normal User	High	IT Manager	System Assurance Manager	Managed by trustea. Tool - Plesk control panel / Putty RDC, Backup Procedure - Manual. Frequency - Weekly (Friday)
			Auditor level - Audit report upload	Auditor	Normal User	Moderate	IT Manager	System Assurance Manager	
			Implementation Partner Level - Entity Support Data management, Activity Management, Monthly IP Tracker Upload, NoC generation for entities	Implementation Partner / Consultants	Normal User	Moderate	IT Manager	System Assurance Manager	
			trustea manager Level - Certification, Decertification, Audit approval, Report generation, CB / IP assignment, Audit Plan approval, Entity profile management, Decertification, VC approval, New membership request management, Report generation	System Assurance Manager / Program Operation Manager / IT Manager	Sub System Admin	High	IT Manager	System Assurance Manager	
			SuperAdmin - User and role management, Certification, Decertification, Audit approval, Report generation, User and role management, Report generation	IT Manager / Director / System Assurance Manager	Admin	High	IT Manager	System Assurance Manager	
			Commercial Partner Level - View dashboard, CB and IP Tracker	Buyer (HUL, TGBL,WB)	Normal User	Moderate	IT Manager	Director	Managed backup service. Backup Frequency - Weekly (Automatic)
			Entity level - Profile management, IP support request, CB selection, Production data upload	Entity	Normal User	Moderate	IT Manager	Program Operation Manager	
	Trustea LMS - eLearning	Learning Section	Trainee Level - Registration, Learning, Examination, Certificate generation	Entity	Normal User	High	IT Manager	System Assurance Manager	Managed backup service. Backup Frequency - Weekly (Automatic)
			Admin Level - Course and Content Development, Examination management, Question paper setting	System Assurance Manager	Normal User	High	IT Manager	System Assurance Manager	

Program	Tool	Sub Tools	Activity	Primary User	Access	Critical	Backup		Alternate PPL/Note
							India (1)	India (2)	
			SuperAdmin - All functions of Admin, User and Role management, and system management.	IT Manager	Admin	High	IT Manager	System Assurance Manager	
		Forum Section	Registered User - Post query, Comment on query	Public	Normal User	Low	IT Manager		
			Admin User - Moderator, Approval Authority	Rajesh / IT Manager	Admin	High	IT Manager	Director	
trustea - General	Office365		Managing trustea's users - Mail + Drive	IT Manager	Admin	High	IT Manager		N/A
	Other Task		IT projects changes/development/tracking of different projects	IT Manager	Admin	Moderate	IT Manager		N/A

APPENDIX B: GLOSSARY OF TERMS

Content	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.
Records	Information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.
Metadata	Metadata is a set of data that describes and gives information about other data. It is a description and context of the data. It helps to organize, find and understand data. Examples of metadata include: • Title anddescription, • Tags andcategories, • Who created andwhen, • Who last modified andwhen, • Who can access orupdate.
Personal Data	The informationrelatestoalivingindividualwhoisidentifiableeither directly from the data itself or from the data in conjunction with other information held bytrustea. Examples of personal data include, but are not limited to: • Name, email, address, home phonenumber • The contents of an individual student file or HRfile • A staff appraisal assessment • Details about lecture attendance or courseworkmarks • Notesofpersonalsupervision,includingmattersofbehaviorand discipline.
Sensitive Personal Data	Sensitive Personal Data (or Special Categories of Personal Data) relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life, criminal convictions or the alleged commission of an offense; trade union membership.
Data	As used in this Policy shall mean information which either: • is Processed by means of equipment operating automaticallyin response to instructions given for thatpurpose; • is recorded with the intention that it should be processed bymeans of such equipment; • isrecordedaspartofaRelevantFilingSystemorwiththeintention that it should form part of a Relevant FilingSystem; • does not fall within any of the above, but forms part of aReadily Accessible record.

	Data, therefore, includes any digital data transferred by computer or automated equipment, and any manual information which is part of a Relevant Filing System.
Data Ownership	A process whereby information/data is assigned to an appropriate owner whose roles and responsibilities in relation to that information/data are clearly documented. This is also deemed to include any data of an academic nature. Acknowledge the nature of the Institute – Refer to the information security policy on controls over creation, transmission, and storage.
Data Classification	A process whereby information/data is classified in accordance with the impact of data being accessed inappropriately, and/or data being lost. The resulting data classification can be associated with a minimum level of control which then needs to be applied when handling data. It is the responsibility of data owners to classify their data.
Data Controller	This means a person or organization who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, Processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organization.
Data Processor	This means a person or organization that holds or Processes Personal Data on the instructions of the Data Controller but does not exercise responsibility for or control over the Personal Data. An employee of a Data Controller, or a School, or Function within an Institute which is Processing Personal Data for the Institute as a whole, is not a Data Processor. However, someone who is contracted by the Data Controller to provide a service that involves the Processing of Personal Data would be a Data Processor. It is possible for one Institute or person to be both a Data Controller and a Data Processor, in respect of distinct sets of Personal Data. It should be noted however that, if you are uncertain as to whether the Institute is acting as a Data Processor or a Data Controller of Personal Data, it should be treated as being the Data Controller (and therefore comply with this Policy in full) until confirmation to the contrary is provided by the ITM or Legal team.
Third-Party	This means an entity, whether or not affiliated with trustea, that is in a businessarrangementwithtrusteabycontract,orotherwise,thatwarrants ongoing risk management. These Third-Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures and otherbusiness arrangements where trustea has an ongoing relationship. Third Party

	relationships, for the purposes of this Policy, generally do not include student or customer relationships. Under GDPR a 'Third Party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller of Data Processor, are authorized to Process Personal Data.
Confidential Data	Includes any data covered by GDPR under the category of personal data. This also includes information considered to be commercially sensitive to the trustea. Examples include strategic plans or intellectual property.
Strictly Confidential Data	Data covered by GDPR under the category of sensitive personal data or special categories of personal data. If this data were to be disclosed to an unauthorized party, it could result in the loss of public confidence, non-compliance with regulatory compliance, legal liabilities and/or additional costs. Special categories under GDPR include audit data, production / SCM data, and growers data.
Data Subject	Refers to the individual to whom Personal Data is held relates, including employees, commercial stakeholders, certification bodies and implementation partners.
Encryption	It is the process of encoding information stored on a device and can add a further useful layer of security. It is considered an essential security measure where personal data is stored on a portable device or transmitted over a public network. Refer to the information Security Policies relating to Information Protection for further Guidance on this area.
Processing	This means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms 'Process' and 'Processed' should be construed accordingly.
Data/Record Retention Schedule	The maximum period of time information/data should be retained by the trustea's for legal and business purposes. It is the responsibility of data owners to define the retention period for their records/data and the eventual fate of the records/data upon completion of this period of time.

All other terms used in this Policy and any documents issued in support of this Policy, not referenced in this section, shall have the same meaning as the GDPR and/or local requirements.

Data description	Source/Producer	Primary owner	Nature of data	Access	Location	Data reviewer	Analysis tool	Purpose/ Insight
Entity Profile	Entity	Enitity	Identity details of entiry	trustea team and respective IP and CB	TCMS, web portal etc	Operation/ program manager	Checklist	To gather raw data for the all future activity
Auditors Approval	Entry by CB auditors	System Assurance Manager	Qualification details	trustea team	TCMS	System Assurance Manager	Checklist	To ensure the qualification and credentials as per trustea's requirement
GAP by IP	Assessment report by IP consultant	System Assurance Manager	Specific clause wise compliance/non compliance	trustea team	TCMS	System Assurance Manager	Checklist	To create the baseline for individual entity
GAP closure report by Entity	No Objection Certificate by IP Consultant	Operation/ program manager	Specific details of actions to close each individual gap	trustea team and respective IP and CB and Entity	TCMS	Operation/ program manager/System Assurance Manager	Checklist	The output of the GAP analysis
Audit report Management	Report by the Certification Body auditors	System Assurance Manager	Quality and accuracy of interpretation along with the supporting evidence	trustea team and respective IP and CB and Entity	TCMS	System Assurance Manager	Checklist	Auditor Evaluation, IP Evaluation, Impact Assessment
System Assurance Audit	System Assurance Audit Report by CB/TSTF	System Assurance Manager	Reverification of third party audit findings and continuous complaince status	trustea team	TCMS	system Assurance Manager/ Director	Graphical analysis of the data	Issue related to continuous compliance MEL/ performance of the CB auditors
Decertification tracker	Decertification audit reports	System Assurance Manager	Specific reasons or caluses elading to decertification	trustea team	TCMS/ Cloud	System Assurance Manager/ Director	Graph and checklist	Analyse the non-conformance pattern

								and make improvement plan Credibility of the assurance system/ performance of the training partners
Volume Tracker	Monthly operation report	Operation/ program manager	Volume data with sectoral analysis	trustea team	TCMS	Operation/ program manager/ Director	Graph and checklist	Certification target achievement and area wise volume, entity type in order to identify any gaps in implementation strategy
Annual Tea Production in India	Tea board website	Operation/ program manager	Monthly, annual tea production in India rea wise/type of prducer wise	Public	Tea board website	Operation/ program manager/ Director	PDF Document	To track the growth of sustainable tea production
IP Performance statistics	IP tracker	Program Manager	IP performance against the Ip performance tracker parameters	trustea team	Cloud folder	Operation/ program manager/ System Assurance Manager/ Director	Graph/ Chart	IP performance
Entity Chronological Journey	tcms	Trustea Team	Time taken at each step of the certifcation journey	trustea team	TCMS	Operation/ program manager/ System Assurance Manager/ Director	Graph and checklist	To analyse the convertion time and take corrective action if

								required
Tracetea Dashboard	Tracetea Application	IT Manager	data of traceteqa compliance like number sof digital diaries, toal kgs through digital traceability,total farmers covered	trustea team, Respective Entity and on demand other relevant stakeholder based on data security protocol	Tracea database / cloud	IT Manager/ Director	Checklist	Analysise the progress of digital traceability
Improvement and compliance statistics data point	audit report	System Assurance Manager	Percentage of complaicne clausewise	trustea team	TCMS	System Assurance Manager/ Director		Verifiable improvement data
Expense details	Tally accounting software owned by trustea	Outsourced Finance Agency	Budget head wise actual spends	trustea, accounting team, statutory auditor	Tally Accounting software	trustea	Tally accounting software owned by trustea	To ensure program continuity by managing expense as per plan and budget
Statutory audit report	Audit Agency	trustea	Item wise complaince on the Indian governement financial legal requirements for companies	in public domain in the Ministry of Corporate Affairs website by payment of nominal fee (approx 1 Euro),	in public domain in the Ministry of Corporate Affairs website, extract of the same is available in trustea website	Statutory Auditor	Chart	Financial transperancy and compliance
Data points for	M&E Reports (LFA) and TCMS Data	System Assurance Manager	Improvement data points to verify actual impact areas.	trustea team	Cloud folder	System Assurance Manager/ Director	MEL Tool made by trustea	To ensure desired output, outcome

M&E	input							and impact in line with trustea's Theory of Change.
Auditors training	Trustea Standard training module	System Assurance Manager	Assessment reports and total training data	System Assurance Manager and IT Manager	Cloud folder/ trustea CBIP training portal	System Assurance Manager/ Director	trustea CBIP training portal	To create the credible task force To ensure credibility of the overall standard implementation
IP Training	Trustea Standard training module	System Assurance Manager	Assessment reports and total training data	System Assurance Manager and IT Manager	Cloud folder/ trustea CBIP training portal	System Assurance Manager/ Director	trustea CBIP training portal	To create the credible task force Help to build compliant entities in terms of sustainable practices
Training on traceability	Tracetea Application and Paper trail	IT Manager/ Program Manager/ IP personnel	Assessment reports and total training data	trustea Team	Tracetea Application / TCMS/ Cloud	IT Manager/ Program Manager	Tracea Application	To create awareness about sustainable production and sourcing within the supply chain who falls under the scope for compliances related to sustainability

STG training	STG Training Module	IP personnel / Program Manager	Assessment reports and total training data	trustea Team	TCMS and Cloud	System Assurance Manager/ Program Manager	Checklist	To create awareness of the applicability of the standard amongst the STGs for all future compliances related to sustainability
trustea E-learning	Trustea e-learning module	System Assurance Manager and IT Manager	Training statistics entity wise and individual trainee wise with assessment statistics	trustea Team	E-learning Portal	System Assurance Manager and IT Manager	Checklist	To create awareness of the applicability of the standard amongst the entities for all future compliances related to sustainability

trustea Sustainable Tea Foundation

6, Southern Avenue,

5th Floor,

Kolkata – 700026, WB, India

Telephone + 919830563511
E-mail dutta@trustea.org, admin@trustea.org