Data Governance Policy

November 2020

Contents

Review History

Date of this Review: 26/11/2020	Date of next review: 26/11/2021

Document Location

Website – Resources > Policies & Guidelines

Review Result

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

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:

- It is the responsibility of each team members and Function to ensure this information is processed in a manner compliant with the relevant data protection legislation and guidance.
- Trustea has an appointed IT Manager ('ITM') who is available to all projects and activities to provide guidance and advice pertaining to this requirement.
- All Staff must appropriately protect and handle information in accordance with the information'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 AND RESPONSIBLITIES

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 it as recommended by the trustea Secretariat. • Ensuring ongoing compliance with the Data Policy in their respective areas of responsibility.

	• Ensuring oversight of data protection issues either through their own work or a Data Protection Oversight Committee or other governance arrangement.
IT Manager	• To lead the data protection compliance and risk management function, with responsibility for advising how to comply with applicable privacy legislation and regulations. • To advise on all aspects of data protection and privacy obligations. • To monitor and review all aspects of compliance with data protection and privacy obligations. • To act as a representative of data subjects in relation to the processing of their personal data. • To report directly on data protection risk and compliance to executive management.
Staff / Stakeholders	• To adhere to policy statements in this document. • 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 Entities Data
- Trustea Staff Data
- Trustea Financial Data
- Trustea Commercial Data
- Trustea Intellectual Property

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:

- Any person who is employed by trustea who receives, handles or processes data in the course of their employment.
- Any external stakeholders of trustea who receives, handles, or processes data in the course of their assignment / activities for administrative, research, certification, facilitation or any other purpose.
- Third party companies (data processors) that receive, handle, or process data on behalf of trustea.
- This applies whether you are working in the trustea, travelling or working remotely.

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, derive benefit from, but also the right to assign these access privileges to others.

In the context of trustea data ownership responsibility will be formally assigned for the following functional domains/process but is not limited to these functions:

- HR
- Trustea Code and training materials
- Entity Certification and audit data
- Entity supply chain and traceability data
- Financial processes
- Resource Planning.

Data ownership responsibilities include:

- Approval of user access
- Approval of user roles/profiles/classes
- Review of access including application data held in network directory locations
- Data classification
- Data retention rules and definition
- Master data changes authorization
- Ensuring availability of information
- Data restoration testing
- Service level management and monitoring.

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 through considering the impact of various risks:

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

Resulting Data Classification	**Confidential Data (+ Strictly Confidential Data)**	**Internal Use Only**	**Public Data**
Data Classification examples	• Finance Data relating to trustea operation and personnel • HR Data • Trustea audit and certification data • Supply chain and production data of certified entities *Strictly Confidential* • *Special Categories of Personal Data .*	• Intranet / Extranet data • Internal telephone books and directories • Financial Budgets	• Public Websites • Campus Maps • Staff Directory

Data that is not yet been classified should be considered **confidential** until the owner assigns the classification.

Confidential Data

Confidential data is information or data protected by statutes, regulations, Institute policies or contractual obligation. 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 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 / Extranet data.
- Internal telephone books and directories.
- Contact, Email address etc

Internal Use only data must be protected to prevent loss, theft, unauthorized access and / or unauthorized 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 web sites
- Publicly-posted press release
- Publicly-posted schedules of classes
- Publicly-posed interactive guidelines, newsletters, newspapers and magazines.

5.1.3 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. POLICY COMPLIANCE

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 Compliance Exceptions

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

6.3 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with the 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 legal action.

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

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	Debasish		In Playstore level only the application is stored. Data is with Cloud 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	Debasish		
			Factory level - weighment, leaf receipt	Factory User	Public User, trustea_admin	High	Debasish		
		tracetea (web app)	Factory Level - Production, Invoice and Warehouse, Salepool management	Factory User	Public User, trustea_admin	High	Debasish		3 Tier application and database are in Cloud server, Backup Procedure - Scheduled / Autobackup, Storage - NICSI DC
			Tea Estate Level - Leaf Collection from garden, collection in factory, production, invoice, warehouse and salepool management	Estate User	Public User, trustea_admin	High	Debasish		
			Advisory/Expert Level - Tracking queries from field, Advisory Help to STG / Estate	Advisor	Public User, trustea_admin	Low	Debasish	Rajesh	
			Buyer / Consignee Level - Tracking Invoice, Backward and Forward Traceability	Buyer (HUL, TGBL,WB)	Public User, trustea_admin	High	Debasish		
			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	Debasish	Rajesh	

Program	Tool	Sub Tools	Activity	Primary User	Access	Critical	Backup		Alternate PPL/Note
							India (1)	India (2)	
		tracetea (SMS Utility)	Message propagation among grower, aggregator, factory, estate and advisor regarding supply chain information	trustea (Auto-generated)	trustea_admin	High	Debasish	Rajesh	Managed service from Rozarpay, Backup Frequency - Alternation day(s)
	trustea - Web portal		Changes on trustea website	Anika / Debasish	Sub System Admin, Admin	High	Debasish	Anika	Managed backup service. Backup Frequency - Weekly (Automatic)
			trustea website back end management	Debasish	Admin	High	Debasish		
	trusteacode - Auditor Desk Portal		Certification Body Level - Audior creation / management, Auditor monitoring	Certification Body	Normal User	High	Debasish	Anandita	Managed by trustea. Tool - Plesk control panel / Putty RDC, Backup Procedure - Manual. Frequency - Weekly (Friday)
			Auditor level - Audit report upload	Auditor	Normal User	Moderate	Debasish	Anandita	
			Implementation Partner Level - Entity Support Data management, Activity Management	Implementation Partner	Normal User	Moderate	Debasish	Anandita	
			trustea manager Level - Certification, Decertification, Audit approval, Report generation	Anandita / Suman	Sub System Admin	High	Debasish	Anandita	
			SuperAdmin - User and role management, Certification, Decertification, Audit approval, Report generation	Rajesh / Anandita	Admin	High	Debasish	Anandita	
	trusteaDBMS		Certification Body Level - Audit Plan management, Entity and STG data management, Verification Certificate [VC] management	Certification Body	Normal User	High	Debasish	Suman	Managed backup service. Backup Frequency - Weekly (Automatic)
			Implementation Partner Level - Monthly IP Tracker Upload, NoC generation for entities	Implementation Partner	Normal User	Moderate	Debasish	Suman	
			trustea manager Level - CB / IP assignment, Audit Plan approval, Entity profile management, Decertification, VC approval, New membership request management, Report generation	Rajesh / Anandita / Suman	Normal User	High	Debasish	Suman	

Program	Tool	Sub Tools	Activity	Primary User	Access	Critical	Backup		Alternate PPL/Note
							India (1)	India (2)	
			Commercial Partner Level - View dashboard, CB and IP Tracker	Buyer (HUL, TGBL,WB)	Normal User	Moderate	Debasish	Suman	
			Entity level - Profile management, IP support request, CB selection, Production data upload	Entity	Normal User	Moderate	Debasish	Suman	
			SuperAdmin - User and role management, Report generation	Debasish	Admin	High	Debasish	Rajesh	
	trusteaLMS - Elearning	Learning Section	Trainee Level - Registration, Learning, Examination, Certificate generation	Entity	Normal User	High	Debasish	Anandita	Managed backup service. Backup Frequency - Weekly (Automatic)
			Admin Level - Course and Content Development, Examination mangement, Question paper setting	Anandita	Normal User	High	Debasish	Anandita	
			SuperAdmin - All functions of Admin, User and Role management, system management.	Debasish	Admin	High	Debasish	Anandita	
		Forum Section	Registered User - Post query, Comment on query	Public	Normal User	Low	Debasish		
			Admin User - Moderator, Approval authority	Rajesh / Debasish	Admin	High	Debasish	Rajesh	
trustea - General	Office365		Managing trustea's users - Mail + Drive	Debasish	Admin	High	Debasish		N/A
	Other Task		IT projects changes/development/tracking of different projects	Debasish	Admin	Moderate	Debasish		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 and description, • Tags and categories, • Who created and when, • Who last modified and when, • Who can access or update.
Personal Data	Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by trustea. Examples of personal data include, but are not limited to: • Name, email, address, home phone number • The contents of an individual student file or HR file • A staff appraisal assessment • Details about lecture attendance or course work marks • Notes of personal supervision, including matters of behavior and 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 offence; trade union membership.
Data	As used in this Policy shall mean information which either: • is Processed by means of equipment operating automatically in response to instructions given for that purpose; • is recorded with the intention that it should be Processed by means of such equipment; • is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System; • does not fall within any of the above, but forms part of a Readily 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 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 nature of Institute – Refer to information security policy on controls over creation, transmission, 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	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	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	Means an entity, whether or not affiliated with trustea, that is in a business arrangement with trustea by contract, or otherwise, that warrants 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 other business 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 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	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 on 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.

trustea Sustainable Tea Foundation

6, Southern Avenue,

5th Floor,

Kolkata – 700026, WB,
India

Telephone + 91 9830563511
E-mail dutta@trustea.org, admin@trustea.org