




Republic of the Philippines
**TECHNICAL EDUCATION AND SKILLS DEVELOPMENT
AUTHORITY**



Data Privacy Manual

Version 1.0 s. 2020

June 03, 2020

	Title: Data Privacy Manual		Document No. TESDA- DPA-01
	Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20 Page: 2 of 58

Document Review and Approval

Version History

Version	Author	Date	Signature	Revision
1.0	Lourdes F. Castante Noemie S. Valois	02.14.2020		Initial draft of the Data Privacy Manual

Approvals

	Name	Date Reviewed/ Approved	Signature
1	Sec. Isidro S. Lapeña	June 3, 2020	
2	DDG Lina C. Sarmiento		
3	Dir. Angelina M. Carreon		



	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 3 of 58

Table of Contents

Executive Summary	4
Overview of Privacy Legislation	5
Definition of Terms	6
Scope and Limitations	10
Further Guidance	11
Data Protection Principles	12
Consents	14
Transfers to Third Parties	15
Disclosures at the Time of Data Collection	16
Processing of Personal Data	18
Security Measures	22
Breach and Security Incidents	28
Inquiries and Complaints	29
Effectivity	31
Appendices	32


	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 4 of 58

1.0 Executive Summary

This Privacy Manual is hereby adopted in compliance with the Data Privacy Act (DPA), its Implementing Rules and Regulations (IRR), and other relevant policies, including issuances of the National Privacy Commission (NPC).

As TESDA respects and values personal data privacy rights, this Manual is intended for TESDA's internal and external operations related to data protection and security measures to mitigate the risks against data breach and reputational damage. The breaches of confidentiality are all about information given out inappropriately. On the other hand, reputational damage may be caused by a hacker that could successfully gain access to sensitive data.

In this regard, this Privacy Manual describes how the personal data must be collected, handled and stored to meet TESDA's data protection standards and in adherence to the general principles of transparency, legitimate purpose, and proportionality.


	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 5 of 58

2.0 Overview of Privacy Legislation

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect personal data in information and communications systems both in the government and the private sector. Therefore, the Technical Education and Skills Development Authority (TESDA) as a government agency which collects personal information from its various clients, is covered by the DPA.

It ensures that entities or organizations which process personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights. A personal information controller (PIC) or personal information processor (PIP) is instructed to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

To inform its personnel of such measures, each PIC (e.g., TESDA) or PIP (e.g., Land Bank for payroll processing) is expected to produce a Privacy Manual. The Manual serves as a guide or handbook for ensuring the compliance of an organization or entity with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the NPC. It also encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization for specific

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 6 of 58

circumstances (e.g., from collection to destruction), directed toward the fulfilment and realization of the rights of data subjects.

3.0 Definition of Terms

For the purpose of this Manual, the following terms are defined, as follows:

- 3.1 “*Act*” refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012;
- 3.2 “*Commission*” refers to the National Privacy Commission;
- 3.3 “*Consent of the data subject*” refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so;
- 3.4 “*Data subject*” refers to an individual whose personal, sensitive personal, or privileged information is processed;
- 3.5 “*Data processing systems*” refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
7 of 58

- 3.6 *“Data sharing”* is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor;
- 3.7 *“Filing system”* refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;
- 3.8 *“Information and communications system”* refers to a system for generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document;
- 3.9 *“Personal data”* refers to all types of personal information;
- 3.10 *“Personal information”* refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
8 of 58

information, or when put together with other information would directly and certainly identify an individual;

3.11 “*Personal data breach*” refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed;

3.12 “*Personal information controller*” refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

3.12.1 A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or

3.12.2 A natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

3.13 “*Personal information processor*” refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;

3.14 “*Processing*” refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
9 of 58

performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system;

3.15 “*Profiling*” refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;


3.16 “*Privileged information*” refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication;

3.17 “*Public authority*” refers to any government entity created by the Constitution or law, and vested with law enforcement or regulatory authority and functions;

3.18 “*Security incident*” is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place;

3.19 “*Sensitive Personal Information*” Sensitive personal information refers to personal information.

3.19.1 About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 10 of 58

3.19.2 About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;

3.19.3 Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

3.19.4 Specifically established by an executive order or an act of Congress to be kept classified.

4.0 Scope and Limitations


4.1 Who is bound by the Manual?

All TESDA personnel, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Data Privacy Manual.

They are responsible for ensuring that:

4.1.1 Any personal data, which they process, is kept securely in accordance with this Data Privacy Manual; and

4.1.2 Personal information is not disclosed accidentally or otherwise to any unauthorized third party.


	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 11 of 58

5.0 Further Guidance

The Section 17 of the NPC Circular No. 16-01, dated October 10, 2016, highlights the importance of Acceptable Use Policy (AUP). It mandates each government agency to have an up-to-date AUP regarding the use by agency personnel of information and communications technology. The policy shall be explained to all agency personnel who shall use such technology in relation to their functions. Each user shall agree to such policy and, for this purpose, sign the appropriate agreement or document, before being allowed access to and use of the technology.

In the same manner, TESDA shall require its personnel to sign an Employee Commitment on the Proper Use of IT Assets vis AUP; beside signing a Non-Disclosure Agreement.


The details about the AUP are explained in Appendix K.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 12 of 58

6.0 Data Protection Principles

TESDA has adopted the following principles to govern its use, collection, and transmittal of Personal Data, except as specifically provided by this Policy or as required by applicable laws:

- 6.1 Personal Data shall only be processed fairly and lawfully.
- 6.2 Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes.
- 6.3 Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed.
- 6.4 Personal Data shall be accurate, complete and current as appropriate to the purposes for which they are collected and/or processed.
- 6.5 Personal Data shall not be kept in a form which permits identification of the Data Subject for longer than necessary for the permitted purposes.
- 6.6 Personal Data shall not be collected or processed unless:
 - 6.6.1 The Data Subject has provided a valid, informed consent. See Section 7;
 - 6.6.2 Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;
 - 6.6.3 Processing is necessary for compliance with TESDA legal obligation;
 - 6.6.4 Processing is necessary in order to protect the vital interests of the Data Subject;

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 13 of 58

6.6.5 Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in TESDA or in a third party to whom the data are disclosed. See Section 8; or

6.6.6 Processing is necessary for legitimate interests of TESDA or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the fundamental rights and freedom of the Data Subject.

6.7 Personal Data shall be collected and processed in accordance with the rights of the Data Subjects. The Data Privacy Act of 2012, Sections 16-18 and its IRR, Sections 34-36 define the data privacy rights of a data subject. The data subject is entitled to right to be informed, right to object, right to access, right to rectification, right to erasure or blocking, right to damages, right to data portability, and right to file a complaint.


6.8 Appropriate physical, technical, and procedural measures shall be taken to:

6.8.1 Prevent and/or to identify unauthorized or unlawful collection, processing, transmittal of Personal Data; and,

6.8.2 Prevent accidental loss or destruction of, or damage to, Personal Data. See Section 11.

* See Appendix A – For Training; Appendix B – For Assessment;


Appendix E- Attendance Sheet; Appendix F -Participant's Profile

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 14 of 58

7.0 Consents

TESDA shall establish a system for the collection and documentation of Personal Data. The Act states that consent is required prior to the collection and processing of all personal data, subject to exemptions provided by the Act and other applicable laws and regulations. The Non-Disclosure Agreement form (See Appendix C) shall conform with the following data privacy requirements:

- 7.1 To be valid, consent must be informed, express, and freely given.
- 7.2 If consent is obtained with other written declarations, the request for consent must be made conspicuous.
- 7.3 Consent with regard to Sensitive Data must refer expressly to those data.
- 7.4 Consent must be revocable.
- 7.5 The consent system shall include provisions for determining what disclosures should or must be made in order to obtain a valid consent, documentation of the date, method and content of the disclosures made, as well as the validity, scope, and volition of the consents given.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 15 of 58

8.0 Transfers to Third Parties

8.1 All transfers of Personal Data to third parties for further processing shall be subject to Data Sharing Agreement. (See Appendix D).

8.2 Personal Data shall not be transferred to another entity, unless reasonable and appropriate steps have been taken to maintain the required level of data protection.

8.3 Personal Data may be communicated to third persons only for reasons consistent with the purposes for which the data were originally collected or other purposes authorized by law.


8.4 All Sensitive Data transferred outside of TESDA or across public communications networks shall be de-identified or shall be protected against unauthorized access by use of encryption.

8.5 Notwithstanding the provisions of Subsections 8.1, Personal Data may be transferred where any of the following apply:

8.5.1 The Data Subject has given consent to the proposed transfer;

8.5.2 The transfer is necessary for the performance of a contract between the Data Subject and TESDA, or the implementation of pre contractual measures taken in response to the Data Subject's request;

8.5.3 The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between TESDA and a Third Party;

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 16 of 58

8.5.4 The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defence of legal claims;

8.5.5 The transfer is required by law;

8.5.6 The transfer is necessary in order to protect the vital interests of the Data Subject; or,


8.5.7 The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

9.0 Disclosures at the Time of Data Collection

9.1 Appropriate disclosures will be made at the time a Data Subject is asked to give consent to the collection or processing of Personal Data, and whenever Personal Data is collected.

9.2 Specific information must be disclosed to the Data Subject and/or any other person from whom Personal Data is obtained at the time of collection, unless the Data Subject already has the information. The business unit collecting the information, in cooperation with the DPO, must establish technical or administrative means for documenting the fact that the Data Subject already has the information and how.

9.3 The foregoing disclosure requirements shall not apply where such disclosure could not be implemented in a reasonable manner with cost and effort

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 17 of 58

proportionate to the importance of the proposed processing, or where applicable law provides an exemption to requirements for disclosure and/or consent.

9.4 If no exemption applies, the following information must be disclosed to the Data Subject and/or any other person from whom Personal Data are obtained at the time of collection:

9.4.1 The address of TESDA, the name and contact details of the DPO or COP.

9.4.2 The purpose(s) of collecting, processing, and transmitting the data (e.g., enrolment)

9.4.3 Whether the source of the data is under an obligation to supply the data and the consequences of failing to do so.


9.4.4 The identities, or at least the categories, of natural or legal persons who will or may receive the data (e.g., TESDA).

9.4.5 The Data Subject's right to access, receive a copy of, erase, and correct the data and the means of exercising those rights.

9.4.6 The Retention period of Personal Data. (refer to Agency's Retention Inventory and Appraisal or NAP Form 1 (See Appendix L).

9.4.7 Procedures available on the process owners in resolving any disputes about processing of the Data Subject's Personal Data.

9.4.8 Any other information necessary to guarantee "fair processing". For example, where the data are to be used in a manner not apparent to the Data Subject, such use should be disclosed.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 18 of 58

9.5 These disclosures should be given as soon as possible, and preferably at the first point of contact with the Data Subject. In the case of employees, the disclosures should be made in the employment contract or appointment. Appropriate disclosures should also be made in any job application form or employee handbook. The disclosures should be made in a manner calculated to draw attention to them.

9.6 The disclosures may be given electronically via online facility or in writing. The receipt or form should be retained along with a contemporaneous record establishing the fact, date, content, and method of disclosure.

9.7 If inadequate disclosures are made initially, additional disclosures may have to be made at a later time, and the fact, date, content, and method of these additional disclosures shall be recorded.

10.0 Processing of Personal Data


10.1 Collection

10.1.1 Collection of personal data shall only be allowed in the following offices:

10.1.1.1 Human Resources Management Division (HRMD) for personnel management and TESDA related activities.

10.1.1.2 Management Information Technology Division (MITD) for the storage and generation of reports from the system.

10.1.1.3 Certification Office (CO) for the assessment and certification of candidates in TESDA-accredited Assessment Centers

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 19 of 58

(ACs) and program registration of the TESDA Technology Institutions (TTIs), public and private TVET providers TESDA Vocational Institutions (TVIs) and ACs.

10.1.1.4 Qualifications and Standards Office (QSO) for technical/industry experts' data sheet and accounts.

10.1.1.5 National Institute for Technical Education and Skills Development (NITESD) for the trainers' profile.

10.1.1.6 NITESD-eTESDA for TESDA Online Program learners and conduct of survey.

10.1.1.7 Scholarship Management Division (SMD) for TESDA scholars' profile.

10.1.1.8 Planning Office (PO) for the conduct of surveys and other related activities like conduct of forum and industry consultations where profiles are collected.

10.1.1.9 Partnership and Linkages Office (PLO) for collecting data from EBT implementers, learners and TESDA partners.

10.1.1.10 Internal Audit Service for the reports of the NISP

10.1.1.11 Provincial and Regional Offices for the profiles of the institutions, training centers, trainers and assessors profile within its jurisdiction.

10.1.1.12 Training Institutions (TTIs and TVIs) for the profile of its learners



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20

Page:
20 of 58

10.1.1.13 Accredited Assessment Centers for the profile of its candidates for national competency assessment.

10.1.1.14 National Inspectorate for Scholarship Programs (NISP) for verification purposes

10.2 Use

10.2.1 The use of personal data shall be allowed by the respective offices identified in Section 10.1.1 including other government agencies (eg. COA, Congress, Senate, etc.) for auditing, reporting, monitoring and budgetary purposes.

10.3 Storage, Retention, Destruction and Disposal

10.3.1 TESDA shall ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing.

10.3.2 TESDA shall always adhere with appropriate security measures in storing collected personal information by using cabinets with locks for hard copies and strict usage of strong passwords for computer-based records.

10.3.3 Permanent records shall be stored in a secure place and its corresponding soft copies shall have back-up files.

10.3.4 Temporary files or records, soft or hard copies like those job applications not accepted, can be disposed of as valueless after a predetermined active period (refer to Agency's RIA- Appendix M).



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
21 of 58

Disposal of hard copies shall follow the disposal policy being followed by the Disposal Committee while the soft copies shall be deleted (refer to Agency's RDS- Appendix M).

10.3.5 Retention period and disposal of all types of personal data collected in Section 10.1 whether hardcopies or electronic copies shall follow the established Retention and Inventory Appraisal (RIA) and Retention and Disposal Schedule (RDS) being handled by the Records Section and that conforms to the quality management system of the agency.


10.3.6 Prior to destruction or disposal of computer hardware or media (e.g., compact discs, memory flash cards, etc.) containing personal data, it shall be checked to ensure that any sensitive data has been removed or securely overwritten.

10.4 Access

10.4.1 Due to the sensitive and confidential nature of personal data, access to it either in computerized systems or in secured filing cabinets shall only be allowed to authorized personnel, for any purpose, except for those contrary to the law, public policy, public order or morals.

10.4.2 Personal data collected as stated in the Section 10.1 shall only be accessed by the authorized personnel in the said office.

10.4.3 The COPs of the respective offices (refer to Section 12.3) that collect personal data shall be assigned as the authorized personnel to access the data. Refer to Section 10.1 of the personal data being collected.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 22 of 58

10.5 Disclosure and Sharing


All TESDA employees shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations. Personal data under the custody of TESDA shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

11.0 Security Measures

In compliance with RA 10173, TESDA shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data. Information security is vital in establishing and sustaining trust between TESDA and its clients - trainees/learners, graduates, assessees, trainers and assessors, institutions with registered programs with TESDA, in maintaining compliance with relevant regulations, and in protecting TESDA's reputation.

The security measures shall guarantee confidentiality that are intended to ensure that the right people can get the sensitive information while avoiding the same from reaching the wrong people. Access must be restricted to those authorized to view the data in question.

Integrity keeps data pure, accurate, trustworthy and consistent by protecting system data from intentional or accidental changes over its entire life cycle. Integrity intends to prevent unauthorized users from making modifications to data or programs,

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 23 of 58

prevent authorized users from making improper or unauthorized modifications, and maintain internal and external consistency of data and programs.

Availability is best ensured by conducting regular hardware preventive maintenance, performing hardware repairs done immediately when needed, functioning operating system environment that is free of software conflicts, keeping current with all necessary system upgrades, providing adequate communication bandwidth and preventing the occurrence of bottlenecks.


11.1 Organizational Security Measures

The human aspect of data protection shall be observed strictly and it shall include the following:

11.1.1 Pursuant to the *TESDA Order No. 168 s. 2020*, the Director-in-Charge of Regional Operations Management Office was assigned as the Data Protection Officer of the agency.

Functions of the DPO. The DPO shall oversee the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.

11.1.2 Functions of the COP. The COP, being an assistant to the DPO, shall perform some of the functions of the DPO.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 24 of 58


11.1.3 Breach Management Team (BMT). The BMT shall regularly convene, at least quarterly, to discuss security measures implemented, being completed, and for those to be employed.

11.1.4 Conduct of Privacy Impact Assessment (PIA). TESDA shall conduct regular Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data to frequently update its existing PIAs.

11.1.5 Recording and documentation of activities carried out by the DPO. The organization shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

11.1.6 Duty of Confidentiality. All employees will be asked to sign a Non-Disclosure Agreement (Appendix C) and Acceptable Use Policy (see Appendix K). All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

11.1.7 Review of Privacy Manual. This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 25 of 58

11.2 Physical Security Measures

To monitor and limit access to the facility containing the personal data, including the activities therein, TESDA shall implement physical security measures. Physical security is about the application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information. It shall provide for the actual design of the facility, the physical arrangement of equipment and furniture, the permissible modes of transfer, and the schedule and means of retention and disposal of data, among others.

11.2.1 Format of data to be collected. Personal data in the custody of TESDA may be in digital/electronic format and paper-based/physical format.

11.2.2 Storage type and location. All personal data in digital or electronic files being processed by TESDA (i.e., including clinical or health data) shall be stored in highly secured computers and external drives for back-up files, where paper-based documents are kept in locked filing cabinets in physically secure offices.

11.2.3 Backup storage devices. HRMD shall control the access to backup storage devices and shall ensure that personal data backed up therein are secured.

11.2.4 Protecting against external and environmental threats. Personal data shall be protected against damage from natural or man-made



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
26 of 58

disaster. To ensure data protection, another copy of backup storage device shall be stored outside the premises of TESDA office, preferably in a safe vault of a bank.


11.2.5 Securing offices, rooms and facilities. Movements inside TESDA shall be recorded using closed-circuit television or CCTV.

11.2.6 Physical entry controls. Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

11.2.7 Design of office space/work station. The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.

11.2.8 Persons involved in processing, and their duties and responsibilities. Persons involved in HR and enrolment processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their personal gadgets or storage devices of any form in their respective offices.

11.2.9 Modes of transfer of personal data within the organization, or to third parties. Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal data.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 27 of 58


11.2.10 Retention and disposal procedure. The Disposal Committee shall retain the personal data of active trainees as indicated in the Retention Inventory and Appraisal and Records Disposition Schedule of TESDA (see Appendix L and M) that conforms in the National Archives of the Philippine (NAP). Upon expiration of such period, the hard copies shall be destroyed and disposed of while its electronic files shall be permanently stored in a secure computer and backup hard drives or compact discs.

11.3 Technical Security Measures

TESDA shall implement technical security measures to make sure that there are appropriate and sufficient safeguards to secure the processing of personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access.

11.3.1 Monitoring for security breaches. HRMD, in coordination with MITD, shall ensure the use of firewall, intrusion detection system to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system.

11.3.2 Security features of the software/s and application/s used. TESDA, through MITD, shall first review and evaluate software applications before the installation thereof in computers and devices of the organization to ensure the compatibility of security features with overall operations.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 28 of 58

11.3.3 Process for regularly testing, assessment and evaluation of effectiveness of security measures. The DPO and COP shall review security policies, conduct vulnerability assessments and penetration testing on a regular schedule.

11.3.4 Encryption, authentication process, and other technical security measures that control and limit access to personal data. Each employee with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication.

12.0 Breach and Security Incidents

Creation of a Breach Management Team (BMT). The BMT shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. If the incident has been confirmed as a data breach of personal data, the DPO shall report it to the NPC within 72 hours.

The BMT shall also execute measures to mitigate the adverse effects of the incident or breach.

The BMT shall comprise the following members who shall be responsible for ensuring immediate action in the event of a security incident or personal data breach.



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
29 of 58


Measures to prevent and minimize the occurrence of breach and security incidents. TESDA shall regularly conduct a Privacy Impact Assessment to identify risks in the processing systems and monitor for security breaches and vulnerability scanning of computer networks if necessary (i.e., vulnerability assessment and penetration testing or VAPT). Personnel directly involved in the processing of personal data must attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the organization.

Procedure for recovery and restoration of personal data. TESDA shall always maintain a backup file for all personal data under its custody. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

Documentation and reporting procedure of security incidents or a personal data breach. The BMT shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to the NPC, within the prescribed period.

13.0 Inquiries and Complaints


Every data subject has the right to reasonable access to his or her personal data being processed by TESDA. Other available rights include: (1) right to dispute the inaccuracy or error in the personal data; (2) right to request the

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 30 of 58

suspension, withdrawal, blocking, removal or destruction of personal data; and (3) right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data. Accordingly, the procedure for inquiries and complaints that will specify the means through which concerns, documents, or forms submitted to TESDA shall be received and acted upon.

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of TESDA, including the data privacy and security policies implemented to ensure the protection of their personal data. They may inquire online (see Appendix I) or write to TESDA at dpo@tesda.gov.ph to briefly discuss the inquiry, together with their contact details for reference.

Complaints shall be filed in three (3) printed copies, or sent to dpo@tesda.gov.ph. The DPO shall confirm with the complainant its receipt of the complaint. From the time the complaints are received, the DPO shall conduct initial evaluations on complaints so received within a reasonable time. Feedback may be expected within 3-5 days working days depending on the result of the evaluations. From here, the entire process, up to final adjudication, should take four to six (6) months.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 31 of 58

If the incident has been confirmed as a data breach of personal data by the BMT, the DPO shall report it to the NPC within 72 hours. The complainant should also be informed that the breach has been reported to NPC as well.

The Appendices I & J show the online data privacy inquiry and complaint forms.

Should there be complaint/s received by offices other than DPO regarding data breach, such complaint/s shall be forwarded by the recipient-office to the DPO for appropriate action, and copy-furnish the complainant.

14.0 Effectivity

The provisions of this Manual are effective this ____ day of _____, 2020, until revoked or amended by TESDA, through a Board Resolution.



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
32 of 58

Appendices

APPENDIX	CONTROL NOS.	DOCUMENT TITLE	REMARKS
Appendix A	TESDA-DPA Form 1	Learners Registration Form (MIS 03-01)	<ul style="list-style-type: none">• Approved by Legal Division• For external use
Appendix B	TESDA-DPA Form 2	TESDA Consent Agreement Form	<ul style="list-style-type: none">• Approved by Legal Division• For external use
Appendix C	TESDA-DPA Form 3	Non-Disclosure Agreement (Data Sharing within the Agency)	<ul style="list-style-type: none">• Approved by Legal Division• For internal use
Appendix D	TESDA-DPA Form 5	Data Sharing Agreement	<ul style="list-style-type: none">• Approved by Legal Division• For external use
Appendix E	TESDA-DPA Form 6	Privacy Disclosure in attendance sheet	<ul style="list-style-type: none">• Approved by Legal Division• For internal use
Appendix F	TESDA-DPA Form 7	Participants Profile	<ul style="list-style-type: none">• Approved by Legal Division• For internal use
Appendix G	TESDA-DPA Form 8	Privacy Policy Statement	<ul style="list-style-type: none">• Approved by Legal Division• For internal/external use
Appendix H	TESDA-DPA WP1	Non-Disclosure Agreement (T2MIS Website)	<ul style="list-style-type: none">• Approved by Legal Division, posted in the T2MIS• For internal/external use
Appendix I	TESDA-DPA Form 9	Online Data Privacy Inquiry Form	<ul style="list-style-type: none">• For inclusion and posting• Approved by Legal Division• For internal/external use
Appendix J	TESDA-DPA Form 10	Online Data Privacy Complaint Form	<ul style="list-style-type: none">• To be developed• Approved by Legal Division• For internal/external use
Appendix K	TESDA-IT Form 1	Acceptable Use Policy (AUP)	<ul style="list-style-type: none">• Approved by Legal Division• For approval and signature of the Secretary• For internal/external use
Appendix L	NAP Form 1	Retention Inventory and Appraisal	<ul style="list-style-type: none">• c/o Records• For internal/external use
Appendix M	NAP Form 2	Records Disposition Schedule	<ul style="list-style-type: none">• c/o Records• For internal/external use
Appendix N		Designation of TESDA Personnel on the Compliance of DPA	<ul style="list-style-type: none">• TESDA Order No. 142 S. 2020



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
33 of 58

APPENDIX A



Technical Education and Skills Development Authority
Pangasiwaan sa Edukasyong Teknikal at Pagpapaulad ng Kasanayan

MIS 03 – 01
(ver. 2020)

Registration Form

LEARNERS PROFILE FORM

I.D. Picture

1. T2MIS Auto Generated

1.1. Unique Learner Identifier
(ULI) Number:

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

1.2. Entry Date: mm/dd/yy

2. Learner/Manpower Profile

2.1. Name:	<input type="text"/> Last Name, Extension Name (Jr., Sr.)	<input type="text"/> First	<input type="text"/> Middle
2.2. Complete Permanent Mailing Address:	<input type="text"/> Number, Street	<input type="text"/> Barangay	<input type="text"/> District
	<input type="text"/> City/Municipality	<input type="text"/> Province	<input type="text"/> Region
	<input type="text"/> Email Address/Facebook Account:		<input type="text"/> Contact No:

3. Personal Information

3.1. Sex

- Male
 Female

3.2. Civil Status

- Single
 Married
 Widow/er
 Separated
 Solo Parent

3.3. Employment Status (before the training)

- Employed
 Unemployed

3.4 Birthdate

<input type="text"/> Month of Birth	<input type="text"/> Day of Birth	<input type="text"/> Year of Birth	<input type="text"/> Age
--	--------------------------------------	---------------------------------------	-----------------------------

3.5 Birthplace

<input type="text"/> City/Municipality	<input type="text"/> Province	<input type="text"/> Region
---	----------------------------------	--------------------------------

3.6 Educational Attainment Before the Training (Trainee)

<input type="checkbox"/> No Grade Completed	<input type="checkbox"/> Pre-School (Nursery/Kinder/Prep)	<input type="checkbox"/> High School Undergraduate	<input type="checkbox"/> High School Graduate
<input type="checkbox"/> Elementary Undergraduate	<input type="checkbox"/> Post Secondary Undergraduate	<input type="checkbox"/> College Undergraduate	<input type="checkbox"/> College Graduate or Higher
<input type="checkbox"/> Elementary Graduate	<input type="checkbox"/> Post Secondary Graduate	<input type="checkbox"/> Junior High Graduate	<input type="checkbox"/> Senior High Graduate

3.7 Parent/Guardian

<input type="text"/> Name	<input type="text"/> Complete Permanent Mailing Address
------------------------------	--



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
34 of 58

4. Learner/Trainee/Student (Clients) Classification:		
<input type="checkbox"/> 4Ps Beneficiary	<input type="checkbox"/> Agrarian Reform Beneficiary	<input type="checkbox"/> Balik Probinsya
<input type="checkbox"/> Displaced Workers	<input type="checkbox"/> Drug Dependents Surrenderers/Surrenderers	<input type="checkbox"/> Family Members of AFP and PNP Killed-in-Action
<input type="checkbox"/> Family Members of AFP and PNP Wounded in-Action	<input type="checkbox"/> Farmers and Fishermen	<input type="checkbox"/> Indigenous People & Cultural Communities
<input type="checkbox"/> Industry Workers	<input type="checkbox"/> Inmates and Detainees	<input type="checkbox"/> MILF Beneficiary
<input type="checkbox"/> Out-of-School-Youth	<input type="checkbox"/> Overseas Filipino Workers (OFW) Dependents	<input type="checkbox"/> RCEF-RESP
<input type="checkbox"/> Rebel Returnees/Decommissioned Combatants	<input type="checkbox"/> Returning/Repatriated Overseas Filipino Workers (OFW)	<input type="checkbox"/> Student
<input type="checkbox"/> TESDA Alumni	<input type="checkbox"/> TVET Trainers	<input type="checkbox"/> Uniformed Personnel
<input type="checkbox"/> Victim of Natural Disasters and Calamities	<input type="checkbox"/> Wounded-in-Action AFP & PNP Personnel	<input type="checkbox"/> Others: _____ (Please Specify)
5. Type of Disability (for Persons with Disability Only): To be filled up by the TESDA personnel		
<input type="checkbox"/> Mental/Intellectual	<input type="checkbox"/> Visual Disability	<input type="checkbox"/> Orthopedic (Musculoskeletal) Disability
<input type="checkbox"/> Hearing Disability	<input type="checkbox"/> Speech Impairment	<input type="checkbox"/> Multiple Disabilities, specify
<input type="checkbox"/> Psychosocial Disability	<input type="checkbox"/> Disability Due to Chronic Illness	<input type="checkbox"/> Learning Disability
6. Causes of Disability (for Persons with Disability Only): To be filled up by the TESDA personnel		
<input type="checkbox"/> Congenital/Inborn	<input type="checkbox"/> Illness	<input type="checkbox"/> Injury
7. Name of Course/Qualification		
8. If Scholar, What Type of Scholarship Package (TWSP, PESFA, STEP, others)?		
9. Privacy Disclaimer		
<i>I hereby allow TESDA to use/post my contact details, name, email, cellphone/landline nos. and other information I provided which may be used for processing of my scholarship application, for employment opportunities and for the survey of TESDA programs.</i>		
<input type="checkbox"/> Agree <input type="checkbox"/> Disagree		
10. Applicant's Signature		
<i>This is to certify that the information stated above is true and correct.</i>		
APPLICANT'S SIGNATURE OVER PRINTED NAME	DATE ACCOMPLISHED	1x1 picture taken within the last 6 months
Noted by:		
_____ REGISTRAR/SCHOOL ADMINISTRATOR (Signature Over Printed Name)	_____ DATE RECEIVED	Right Thumbmark



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
35 of 58

APPENDIX B

TESDA-DPA Form 2

TESDA CONSENT AGREEMENT FORM

(Assessment)

Do you authorize the Technical Education and Skills Development Authority (TESDA) to share your career information (such as Full Name, NC/COC Certificate No., NC/COC Qualification Details, Date of Issuance, Contact Details and ID Pictures) with any legitimate party for the following purposes:

- Research
- Training
- Employment
- Advocacy


Kindly check your preference and sign over your printed name below.

Yes, I want to share my career information and I expressly give my consent thereto

No, I don't give my consent and I want my career information to be restricted only for TESDA's Use and profiling purpose only

Signature over Printed Name

Date: _____

	Title: Data Privacy Manual		Document No. TESDA- DPA-01
	Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20
			Page: 36 of 58

APPENDIX C

TESDA-DPA Form 3

NON – DISCLOSURE AGREEMENT *(Data Sharing Agreement within the Agency)*

TESDA, being a government agency which collects, processes and stores personal information, including those from clients in its various projects and programs, adheres to the Republic Act No. 10173, otherwise known as the “Data Privacy Act of 2012”

Accordingly, any TESDA personnel undertakes not to use the personal information disclosed by the Learners/Candidates for any purposes other than that set by TESDA nor disclose it to any third party. Any disclosure, sharing or transfer of the personal information shall only be allowed with the express consent of the Learner/Candidate provided the purpose thereof is clarified.

The undertakings above apply to all of the information disclosed, regardless of the way or form in which it is disclosed or recorded.

The parties shall ensure that each member of the staff of the parties, whether permanently or contractually employed, having access to or being involved in performing the Services, undertakes a duty of confidentiality and is formed of and complies with the obligations of this Non-Disclosure Agreement.”

I Agree

I Disagree

TRANSFeree:

Name: _____

Signature: _____

Office / Division: _____

Date: _____

REQUEST:

APPROVED BY:

HEAD OF THE OFFICE

DATE



Title: Data Privacy Manual		Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 37 of 58

APPENDIX D

TESDA-DPA Form 5

DATA SHARING AGREEMENT

Data requester (“Transferee”) has asked TESDA to provide copies of the _____ . (See attached documents for Data requested by the Transferee.) TESDA agrees to provide Transferee with the requested Data, under the terms of this Data Sharing Agreement.

1. The Transfer of Data is not and shall not be deemed a sale. The data are instruments of service. TESDA shall be deemed the Data’s author and shall retain all propriety rights, including any copy rights, embodied therein.
2. Transferee may transfer the data to its _____ (collectively “Others”). Provided Transferee requires the Others to be bound by this Agreement as if they were the Transferees in this Agreement. Transferees and Others may use the Data only for purposes related to this Projects.
3. The Data are furnished “as is”. TESDA makes no representations or warranties, express or implied, of the Data’s merchantability or fitness for a particular purpose, with respect to the Data’s quality, adequacy, completeness, or sufficiency, or as to any results to be achieved by the Data’s use or the Data’s conformance with the as-built conditions.
4. Transferee acknowledge that anomalies and errors may occur when the Data is transferred electronically or used in an incompatible computer environment. Transferee solely accepts the risk associated with, and the responsibility for, any damages to hardware, software computer systems, or networks related to the Data’s transfer or use. TESDA Shall have no responsibility to provide software or training to allow Transferee to use Data.
5. Transferee agrees to indemnify, defend and hold TESDA., its offices, directors, employees, agents, and consultants harmless from and against any and all claims, liabilities, suits, demands, losses, damages, costs, and expenses including but not limited to, reasonable attorney’s fees and all legal expenses and fees incurred through appeal, and all interest thereon, occurring to or resulting from any all persons, firms or any other legal entities on account of any damages or losses to property or persons, including, but not limited to, injuries, death or economic losses, arising out of Transferees’ or Others’ use, reuse, transfer, or modification of the Data, except where a court or forum of competent jurisdiction determines TESDA is solely liable for such damages or losses.



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20

Page:
38 of 58

6. If transferee fails to perform or observe any of the terms of this Data Sharing Agreement, TESDA may demand, and Transferee immediately shall return, the Data and any copies thereof.
7. In any legal proceeding to enforce this Agreement, the prevailing party shall be entitled to recover its reasonable attorneys' fee ad costs of defense.

AUTHORIZATION:

_____ :

Name: _____

Signature: _____


Date: _____

TESDA:

Name:

Signature: _____

Date: _____

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 39 of 58

LIST OF DATA REQUESTED

(NOTE: the data below are example only, kindly indicate the data you are requesting)

Type of Request:

I. Regarding Students


General Information

- Name (Family Name, First Name, Middle Name/Middle Initial)
- Complete Address
- Email Address
- Contact Number
- Birth Date
- Age

II. Employment

General Information

- Name (Family Name, First Name, Middle Name/Middle Initial)
- Complete Address
- Email Address
- Contact Number
- Birth Date
- Date of Employment
- Name of Company

	Title:		Document No.
	Data Privacy Manual		TESDA- DPA-01
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 40 of 58

APPENDIX E

TESDA-DPA Form 6



TECHNICAL EDUCATION AND SKILLS DEVELOPMENT AUTHORITY

<Office>

<Division>

ATTENDANCE SHEET

<Title of Event>

<Date, Venue>


	NAME	SEX	DESIGNATION	OFFICE/DIVISION	CONTACT NO.	EMAIL ADD	SIGNATURE

Noted by:

Name and Signature

Division Head

PRIVACY DISCLAIMER: In compliance to the R.A. 10173 otherwise known as the "Data Privacy Act of 2012". The <Office-Division> secretariat shall collect and process your Personal Information provided for the purpose of documentation of the program conducted. Rest assured that the team shall maintain the integrity and confidentiality of your Personal Information as mandated by

	Title: Data Privacy Manual	Document No. TESDA- DPA-01
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20
		Page: 41 of 58

APPENDIX F

TESDA-DPA Form 7



TECHNICAL EDUCATION AND SKILLS DEVELOPMENT AUTHORITY

Regional Operations Management Office

Management Information Technology Division

4th Flr. TESDA Main Building, TESDA Complex, Taguig City

PARTICIPANT'S PROFILE

Title of the Program	
Venue	
Duration/Schedule of the Program	

PERSONAL INFORMATION			
NAME <i>(Please write in CAPITAL LETTERS)</i>			
Surname			
First Name			
Middle Name			
Nickname			
Mobile No.:			
E-mail Add.:		Contact No.:	
Residential Add.:			
Date of Birth		Age	
Sex <input type="checkbox"/> Male <input type="checkbox"/> Female	Civil Status <input type="checkbox"/> Single <input type="checkbox"/> Separated <input type="checkbox"/> Married <input type="checkbox"/> Widow/er		
EDUCATIONAL BACKGROUND			
Highest Educational Attainment/Completed:			
<input type="checkbox"/> Vocational	<input type="checkbox"/> College Graduate	<input type="checkbox"/> Post Graduate	
Course/Degree			



Title: Data Privacy Manual		Document No. TESDA- DPA-01
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20
		Page: 42 of 58

IT RELATED TRAINING/ COURSES ATTENDED (within 3 years)

Title	Training Duration	Conducted/Sponsored by:


EMPLOYMENT INFORMATION

Name of Institution	
Adress of Institution	
Contact No.	
Position	

PRIVACY DISCLAIMER: In compliance to the R.A. 10173 otherwise known as the "Data Privacy Act of 2012". The <Office-Division> secretariat shall collect and process your Personal Information provided for the purpose of documentation of the program conducted. Rest assured that the team shall maintain the integrity and confidentiality of your Personal Information as mandated by the law.

(Signature over Printed Name)

Date Accomplished

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 43 of 58

APPENDIX G

TESDA-DPA Form 8

PRIVACY POLICY STATEMENT

(For TESDA Central Office, Regional and Provincial Offices, and TTIs)

To our Valued Stakeholders


Your personal data and privacy are important to us. We, at Technical Education and Skills Development Authority, are committed to protect and implement appropriate security procedures to maintain the integrity and confidentiality of your personal data in compliance with the Republic Act 10173 otherwise known as “**Data Privacy Act of 2012.**”

The agency will only collect personal data that you provided to us voluntarily. By providing us with your personal data and signing the consent form provided, you authorized the Agency, our Personal Information Controllers (PICs) to collect, process, use and transfer your Personal Information in order to receive service/s, and programs provided by the agency.

The agency stores data in the system/server with appropriate security to avoid data breach. Transfer of personal data may only be done by the authorized Administrator for the purposes of reports generation. Otherwise, personal data shared/transferred to third parties for further processing shall be subject to Data Sharing Agreement (DSA) The agency DSA adheres to the principle of DPA.

For inquiries regarding our Privacy Policy Statement and the processing of your personal data, please coordinate with ROMO at 886-7679 / 777-1231.

SEC. ISIDRO S. LAPEÑA, PhD., CSEE
 Director General

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 44 of 58

APPENDIX H



TESDA-DPA - WP1

NON – DISCLOSURE AGREEMENT

TESDA, being a government agency which collects, processes and stores personal information, including those from clients in its various projects and programs, adheres to the Republic Act No. 10173, otherwise known as the “Data Privacy Act of 2012”

Accordingly, any TESDA personnel undertakes not to use the personal information disclosed by the Learners/Candidates for any purposes other than that set by TESDA nor disclose it to any third party. Any disclosure, sharing or transfer of the personal information shall only be allowed with the express consent of the Learner/Candidate provided the purpose thereof is clarified.

The undertakings above apply to all of the information disclosed, regardless of the way or form in which it is disclosed or recorded.

The parties shall ensure that each member of the staff of the parties, whether permanently or contractually employed, having access to or being involved in performing the Services, undertakes a duty of confidentiality and is formed of and complies with the obligations of this Non-Disclosure Agreement.”

I Agree and Continue

Reply to email

Dear T2MIS User,

This is to confirm that you read and understood the TESDA PIC Contract Agreement.

Sincerely,

T2MIS Administrator
MITD-ROMO



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
45 of 58**APPENDIX I**

TESDA-DPA Form 9

ONLINE DATA PRIVACY INQUIRY FORM

Privacy Inquiry: To contact TESDA' Privacy team regarding a data privacy-related question, comment, or issue, please enter your contact details and question here.

We will only use the information you provide to respond to your inquiry, and for statistical analysis and reporting.

First Name

Surname

Email (required)

This is the email address we will use to reply to you.

Confirm email (required)

Phone Number


What is your question? (required)

Additional Information (if any)

If you would like to add any information to clarify your inquiry include it here.

SUBMIT

CANCEL INQUIRY

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20
		Page: 46 of 58

APPENDIX J

TESDA-DPA Form 10

ONLINE DATA PRIVACY COMPLAINT FORM

TESDA complies with Data Protection Act of 2012. This privacy law regulate how personal information is handled throughout its lifecycle, from collection to use and disclosure, storage, accessibility and disposal.

Complaint should be made within 6 months from the time you became aware of the alleged breach.

You can lodge a complaint about an alleged breach of your privacy by using the online form below.

For your privacy and security, we use end-to-end encryption to securely transmit your submission to us. Nothing you enter is stored on our website which also means that you cannot save as you go, for example to resume later. After you have submitted the form, you will be able to print an onscreen confirmation of what you submitted, for your records.

We recommend that you only lodge your complaint from a trusted computer such as your own. For your privacy and security, we do not recommend you use a public computer (e.g. from an internet cafe) or your employer's computer, or lodge it using public wi-fi.

If you want to be certain that a breach has been committed before filing a complaint, kindly send us an inquiry using the online Data Privacy Inquiry Form. If you need any help, call our inquiries line (886-7679 / 777-1231, 8:00am-5:0pm).

We will use the information you submit to investigate your complaint. If you wish to access or correct this information, please let us know.

If you have a concern or complaint about the handling of your personal information, please complete this complaint form and send to dpo@tesda.gov.ph.

Collection, Use and Disclosure of your Personal Information

In the course of submitting this form, you are providing personal information. Your personal information will be managed in accordance with the TESDA Data Privacy Manual.

- To make a complaint, we require your name and a method of contacting you (preferably an email address or postal address).
- Your personal information is collected on this form to assist the TESDA' Office of the Data Protection Officer (DPO) to respond to your concerns.
- You are welcome to contact the office of the DPO anonymously to make an inquiry or discuss privacy issues. However, if you do not wish to provide your personal information, the DPO office may be limited in the assistance it is able to provide to you.
- Details of the complaint may be conveyed to the individuals named in the complaint, so that the substance of the complaint can be appropriately investigated. Details may also be disclosed to other parties who may have information relevant to the complaint and its investigation.
- You may gain access to a copy of your personal information by making a request.



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
47 of 58

YOUR COMPLAINT

SECTION 1 – YOUR CONTACT DETAILS

Title:	<input type="checkbox"/> Mr	<input type="checkbox"/> Ms	<input type="checkbox"/> Mrs	<input type="checkbox"/> Miss
	<input type="checkbox"/> Other, please specify			
Full Name:				
Postal Address: (if applicable)				
Email:				
Phone: (if applicable)				
Preferred method of contact:	<input type="checkbox"/> Telephone	<input type="checkbox"/> Mobile	<input type="checkbox"/> Email	<input type="checkbox"/> Mail

SECTION 2 – COMPLAINT DETAILS - The clearer your explanation is, the more easily we will be able to assist you. Please feel free to attach additional information.

Date issue occurred	/ /	Date you became aware of the issue	/ /
---------------------	-----	------------------------------------	-----

Personal information involved

<input type="checkbox"/> Name	<input type="checkbox"/> Email Address	<input type="checkbox"/> Username
<input type="checkbox"/> ID Number	<input type="checkbox"/> Telephone Number	<input type="checkbox"/> Home Address
<input type="checkbox"/> Date of Birth		
<input type="checkbox"/> Other, please specify		

Sensitive Information involved

<input type="checkbox"/> Racial or Ethnic Origin	<input type="checkbox"/> Political Opinions	<input type="checkbox"/> Membership of a political association
<input type="checkbox"/> Religious beliefs or affiliations	<input type="checkbox"/> Philosophical beliefs	<input type="checkbox"/> Membership of a professional or trade association
<input type="checkbox"/> Membership of a trade union	<input type="checkbox"/> Sexual preferences or practices	<input type="checkbox"/> Criminal record



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
48 of 58

In what way was your privacy compromised?

Describe accurately the details of your complaint.

Who was involved? (include names of individuals involved if known)

How did you become aware of the issue?

Other

SECTION 3 – Supporting Information

Attach copies of any supporting documents relative to your complaint.

SECTION 4 – What Resolution are you Seeking?

What are you seeking from TESDA to resolve your complaint?

SECTION 5 – Sign and Date

Your signature

Date

Return your completed form to

Email: dpo@tesda.gov.ph

We will acknowledge receipt of your complaint. You do not need to do anything further until the DPO contacts you.



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
49 of 58**APPENDIX K**

TESDA-IT Form 1

**ACCEPTABLE USE POLICY FOR INFORMATION TECHNOLOGY (IT)
RESOURCES****I. OVERVIEW**

The Acceptable Use Policy (AUP) is intended to outline expected behaviour in regards to the use of Government information technology (IT) resources and to delineate between authorized and unauthorized operating practices. The AUP also provides an overview of IT system security policy mandated by TESDA. All Government IT resources, including but not limited to, hardware, software, storage media, and computer and network accounts, provided by TESDA are the property of TESDA. They are to be used for business purposes in serving the interests of the Government and TESDA customers in the course of normal operations. Use of Government IT resources for purposes other than those identified within this policy are strictly prohibited and could negate the security of TESDA IT systems. Effective security is a team effort involving the participation and support of everyone who deals with information and/or information systems. It is the responsibility of everyone to know these guidelines, and to conduct their activities accordingly.

II. SCOPE


This policy applies to all personnel employed by TESDA whether permanent or non-permanent, contract of service, job orders, including its trainees as well as contractors/vendors who are authorized to use TESDA-owned IT facilities and resources. This policy covers the proper use of IT facilities and resources of TESDA, which includes all IT equipment, software, accessories, networking facilities and services whether central or remote, and most importantly, the resulting data and information generated from it.

III. POLICY**A. Network Resources**

1. **Access Privilege.** All qualified users of TESDA IT resources shall be issued a unique login name and password to gain access to network resources.
2. **Passwords.** Refer to the TESDA Circular on the Implementing IT Policies and Guidelines.
3. **Username.** It is the responsibility of the employee to ensure that his/her password remains secret and secure. The employee shall not share it with other individuals. The exception is when an employee surrenders his/her password if requested to do so in the presence of his/her supervisor.
4. **Security and Responsibility.** The Agency reserves the right to hold the employee liable for damages caused by the employee's failure to protect the confidentiality of his/her password in accordance with the above guidelines.

Prohibitions:


1. Sending or sharing with unauthorized persons of any information that is confidential.
2. Installing software that has not been authorized by the Management Information Technology Division (MITD) of the Agency.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 50 of 58

3. Using network resources to play or download games, music or videos that are not in support of business functions.
4. Leaving workstation unattended without any password.
5. Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
6. Reconfiguration of any TESDA-approved VPN technology by any users, other than the system administrators performing official duties to ensure that mandated security requirements are not inadvertently disabled or modified.
7. Using network resources in support of unlawful activities as defined law.
8. Utilizing network resources for activities that violate conduct policies established by the Human Resource Management Division (HRMD) or the Agency where the user is employed or under contract.

B. E-mail

1. **TESDA E-mail Privileges.** TESDA grants e-mail accounts to its employees, subject to the following conditions:
 - 1.1 The employee shall not use e-mail for illegal, immoral or any purpose/s disallowed by TESDA.
 - 1.2 Users shall be responsible in maintaining his/her files.
 - 1.2.1 Granted official users email accounts shall be used for official purposes only;
 - 1.2.2 The Google Apps Administrator of the Regional Offices and LMID-Planning Office shall be responsible for the activation and deactivation of the email accounts granted to the regions and central office, respectively;
 - 1.2.3 List of new/retired/resigned employees shall be provided by the Administrative Services to the administrator for activation/deactivation of their accounts;
 - 1.2.4 Users are advised to manage their individual and office email accounts and shall observe the following:
 - 1.2.4.1 Display their signature email for reference purposes
 - Name:*
 - Designation:*
 - Office Address:*
 - Contact Number:*
 - 1.2.4.2 Control in the number of emails stored in an account.
 - 1.2.4.2.1 Maintain only all relevant emails necessary for your profession and unsubscribe to unwanted promotional emails
 - 1.2.4.3 Maintenance of Spam, Trash, Draft, Sent Mail and Inbox
 - 1.2.4.4 In case of retirement, separation or end of contract:
 - 1.2.4.4.1 Retrieve and turnover of important files and documents shall be done within 5 working days to their immediate supervisor
 - 1.2.4.4.2 Advisory shall be issued to all related partners and stakeholders on the effectivity on the deactivation of the users account.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 51 of 58

2. **Responsibility of Maintenance.** The MITD shall be responsible of giving the e-mail privileges however, the users are responsible for maintaining the security of their TESDA e-mail account and to take precautions to prevent unauthorized access to their mailbox.

Prohibitions:

1. Sending unsolicited junk email or chain letters (e.g. “spam”) to any users of the network.
2. Clicking or following any hyperlinks or URL’s included in an unsolicited e-mail message.
3. Sending any material that contains viruses, Trojan horses, worms, time bombs, cancel bots, or any other harmful or deleterious programs.
4. Sending copyrighted materials via email that is either not within the fair use guidelines or without prior permission from the author or publisher.
5. Sending or receiving communications that violate conduct policies established by the Human Resources Management Division or the Agency where the user is employed or under contract.
6. Sending confidential material to an unauthorized recipient, or sending confidential e-mail without the proper security standards (including encryption if necessary) being met.

C. Workstations.

1. All laptop computers, hardware, or software are assigned to users on an individual basis. Users must take every reasonable precaution to protect such resources from loss or damage.
2. Users must not change any security settings on their workstation.
3. Users must never leave their workstations unattended and unprotected without the utilization of a manual (Ctrl-Alt-Delete) password-protected screensaver.
4. Users must not clear the application, security or system event logs.


IV. PRIVACY EXPECTATIONS.

Employees do not have a right, nor should they have any reasonable expectation, of privacy while using any Government IT resources at any time, including accessing the Internet or using e-mail. To the extent that employees wish that their private activities remain private, they should avoid using Government IT resources such as their TESDA-issued computer, the Internet access, or e-mail for such activities.

By using Government IT resources, employees give their consent to disclosing the contents of any files or information maintained using this equipment. In addition to access by TESDA officials, data maintained on Government IT resources may be subject to discovery and Freedom of Information Act requests. By using Government office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet or using e-mail. Any use of Government telecommunications resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

V. CONSEQUENCES OF NON-COMPLIANCE

Violations of policies and procedures may result in disciplinary actions.

	Title: <p style="text-align: center;">Data Privacy Manual</p>	Document No. TESDA- DPA-01	
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20	Page: 52 of 58

VI. WAIVER

1. **Loss of Data.** Users recognize that systems and networks are imperfect and waive any claim for lost work or time that may arise from the use of the IT System. The Agency shall not be liable for degradation or loss of personal data, software, or hardware as a result of their use of the IT System.
2. **Authorization.** Users recognize that TESDA provides access to the IT System only as a privilege and not a right; that they have no right to use it for any purpose other than those directly connected with the work of TESDA; and that TESDA may take whatever measures it deems necessary to enforce this. Users therefore waive any action they may have against TESDA under any law or administrative rule or regulation for any act the TESDA undertakes under this Policy.

EMPLOYEE'S COMMITMENT

VERIFIED BY DPO

Name and Signature

Name and Signature



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20

Page:
53 of 58

APPENDIX L

Records Inventory and Appraisal (NAP Form 1)

NATIONAL ARCHIVES OF THE PHILIPPINES <i>Pambansang Sinupan ng Pilipinas</i> RECORDS INVENTORY AND APPRAISAL		AGENCY				ORGANIZATIONAL UNIT			TELEPHONE NO.:			
RECORDS SERIES TITLE & DESCRIPTION		PERIOD COVERED		VOLUME IN CUBIC METER	LOCATION OF RECORDS	FREQUENCY OF USE	DUPLICATION	TIME VALUE T / P	UTILITY VALUE Adm / F / L / Arc	RETENTION PERIOD		DISPOSITION PROVISION
									Adm	Fiscal	Legal	

LEGEND:

TIME VALUE: T - Temporary P - Permanent

UTILITY VALUE: Adm - Administrative F - Fiscal L - Legal Arc - Archival

PREPARED BY:

ASSISTED BY:

APPROVED BY:

Name and Position

NAP Records Management Analyst

Chief of the Division/Department



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20

Page:
54 of 58

APPENDIX M

Records Disposition Schedule (NAP Form 2)

NAP Form No. 2
2008

NATIONAL ARCHIVES OF THE PHILIPPINES <i>Pambansang Sinupan ng Pilipinas</i> RECORDS DISPOSITION SCHEDULE		1. AGENCY NAME:			
		2. ADDRESS:			
3. SCHEDULE NO.:		4. DATE PREPARED:			
5. ITEM NO.	6. RECORD SERIES TITLE AND DESCRIPTION	7. RETENTION PERIOD			8. REMARKS
		Active	Storage	Total	

IMPORTANT: Pursuant to Section 18, Article III, RA 9470 s. 2007, "No government department, bureau, agency and instrumentality shall dispose of, destroy or authorize the disposal or destruction of any public records, which are in the custody or under its control except with the prior written authority of the executive director."



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20

Page:
55 of 58

NAP Form No. 2
2008

9. Prepared by: _____ Name _____ Position	11. Recommending Approval: _____ Name _____ Position
10. Assisted by: _____ Name _____ Position	12. Approved: _____ Name _____ Position
TO BE ACCOMPLISHED BY THE NATIONAL ARCHIVES OF THE PHILIPPINES	
<p>This Records Disposition Schedule</p> <p><input type="checkbox"/> is being returned for improvement / correction</p> <p><input type="checkbox"/> is being recommended for approval</p> <p>_____ Chairman Records Management Evaluation Committee</p> <p>_____ Date</p> <p style="text-align: right;">APPROVED:</p> <p style="text-align: right;">_____ Executive Director</p> <p style="text-align: right;">_____ Date</p>	



Title: Data Privacy Manual		Document No. TESDA- DPA-01
Prepared by: ROMO - MITD	Approved by:	Date Issued: 6.03.20 Page: 56 of 58

APPENDIX N

TESDA Order No. 142 S. 2020 “Designation of TESDA Personnel on the Compliance of Data Privacy Act”

TESDA ORDER

SUBJECT: DESIGNATION OF TESDA PERSONNEL ON THE COMPLIANCE OF DATA PRIVACY ACT		No. <u>142</u> s. 2020 Page <u>1</u> of <u>3</u> pages
Date Issued: February 20, 2020	Effectivity: As Indicated	Supersedes: TESDA Order No. 44 & 278 Series of 2017
<p>In the interest of the service and in compliance with the Republic Act No. 10173, otherwise known as the “Data Privacy Act of 2012”, the following TESDA Officials and Employees are hereby designated to the identified positions:</p>		
Data Privacy Officer (DPO)	Deputy Director General, <i>TESDA Operations (TESDO)</i>	
Compliance Officer for Privacy (COP)	<p><i>For the Central Office</i></p> <ul style="list-style-type: none"> Director-in-Charge, <i>Regional Operations Management Office (ROMO)</i> <p><i>For the Regional Offices</i></p> <ul style="list-style-type: none"> Regional Directors Provincial/ District Directors 	
Personal Information Controllers (PIC) for Central Office	<ul style="list-style-type: none"> Chief TESD Specialist, <i>Human Resource Management Division (HRMD-AS)</i> Chief TESD Specialist, <i>Procurement Division (PD-AS)</i> Information Technology Officer III, <i>Management Information Technology Division (MITD-ROMO)</i> Chief TESD Specialist, <i>eTESDA (eTESDA-NITESD)</i> Chief TESD Specialist, <i>Scholarships Management Division (SMD-ROMO)</i> Chief TESD Specialist, <i>Competency Programs and Systems Development Division (CPSDD-QSO)</i> Chief TESD Specialist, <i>Policy Research and Evaluation Division (PRED-PO)</i> Chief TESD Specialist, <i>Program Registration Division (PRD-CO)</i> Chief TESD Specialist, <i>Competency Assessment Division (CAD-CO)</i> Chief TESD Specialist, <i>Partnership and Linkages Division (PND-PLO)</i> Chief TESD Specialist, <i>Public Information Division (PID-ODG)</i> 	
Personal Information Controllers (PIC) for Regional Offices	<ul style="list-style-type: none"> Chief TESD Specialist, <i>Regional Operations Division (ROD)</i> Chief Administrative Officer, <i>Financial & Administrative Service Division (FASD)</i> Processing Officers, <i>TESDA Training Institutions (TTIs)</i> 	
Breach Management Team (BMT) Chairperson	Deputy Director General, <i>TESDA Operations (TESDO)</i>	
Breach Management Team Co-Chairperson	Director-in-Charge, <i>Regional Operations Management Office (ROMO)</i>	
BMT Members	<ul style="list-style-type: none"> Executive Director, <i>Administrative Service (AS)</i> Executive Director, <i>Certification Office (CO)</i> Executive Director, <i>Qualifications and Standards Office (QSO)</i> Executive Director, <i>Partnership and Linkages Office (PLO)</i> Executive Director, <i>Planning Office (PO)</i> Executive Director, <i>National Institute for Technical Education and Skills Development (NITESD)</i> Executive Director, <i>Financial and Management Service (FMS)</i> 	
<p>Functions of DPO:</p> <ol style="list-style-type: none"> Implement reasonable and appropriate organizational, physical and technical measures intended for the personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing 		



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
57 of 58**TESDA ORDER**

SUBJECT: DESIGNATION OF TESDA PERSONNEL ON THE COMPLIANCE OF DATA PRIVACY ACT		No. <u>142</u> s. 2020 Page <u>2</u> of <u>3</u> pages
Date Issued: February 20, 2020	Effectivity: As Indicated	Supersedes: TESDA Order No. 44 & 278 Series of 2017
<ol style="list-style-type: none">2. Implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental, loss or destruction and human dangers such as unlawful processing3. Determine the appropriate level of security by taking into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation <p>Functions of COP:</p> <ol style="list-style-type: none">1. Monitor the Personal Information Controllers or Personal Information Processors compliance with the Data Privacy Act;<ul style="list-style-type: none">• collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;• analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;• inform, advise, and issue recommendations to the PIC or PIP;• ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and• advise the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;2. Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;3. Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);4. Ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the DPO and to the Breach Management Team of the reports and other documentation concerning security incidents or data breaches within the prescribed period;5. Inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP;6. Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;7. Serve as the contact person of the PIC or PIP vis-à-vis data subjects concerning data privacy or security issues;8. Cooperate, coordinate and seek advice from the DPO and regarding matters concerning data privacy and security; <p>Functions of PIC:</p> <ol style="list-style-type: none">1. Effectively communicate to its personnel, the designation of the DPO or COP and his or her functions;2. Allow the DPO or COP to be involved from the earliest stage possible in all issues relating to privacy and data protection;3. Provide sufficient time and resources (financial, infrastructure, equipment, training, and staff) necessary for the DPO or COP to keep himself or herself updated with the developments in data privacy and security and to carry out his or her tasks effectively and efficiently;4. Grant the DPO or COP appropriate access to the personal data it is processing, including the processing systems;5. Where applicable, invite the DPO or COP to participate in meetings of senior and middle management to represent the interest of privacy and data protection;6. Promptly consult the DPO or COP in the event of a personal data breach or security incident; and7. Ensure that the DPO or COP is made a part of all relevant working groups that deal with personal data processing activities conducted inside the organization, or with other organizations. <p>Functions of BMT:</p> <ol style="list-style-type: none">1. Implement the security incident management policy of the agency2. Manage the security incidents and personal data breaches, including the conduct of initial assessment of the incident or breach in order to ascertain the nature and its extent;3. Responsible for ensuring immediate action in the event of a security incident or personal data breach.		



Title:

Data Privacy Manual

Document No.

TESDA- DPA-01

Prepared by:
ROMO - MITD

Approved by:

Date Issued:
6.03.20Page:
58 of 58**TESDA ORDER**

SUBJECT: DESIGNATION OF TESDA PERSONNEL ON THE COMPLIANCE OF DATA PRIVACY ACT		No. <u>141</u> s. 2020 Page <u>3</u> of <u>3</u> pages
Date Issued: February 20, 2020	Effectivity: As Indicated	Supersedes: TESDA Order No. 44 & 278 Series of 2017

4. Manage the agency compliant with the relevant provisions on the personal data breach management.

The MITD-ROMO shall function as Secretariat to assist the **DPO and Breach Management Team** in performing their functions/responsibilities.

This Order supersedes TESDA Order Numbers 44 and 278 s. 2017 regarding the designation of the Data Protection Officers and creation of Technical Working Committee for TESDA Information Security.

This Order takes effect as indicated.


SEC. ISIDRO S. LAPEÑA, PhD., CSEE
Director General