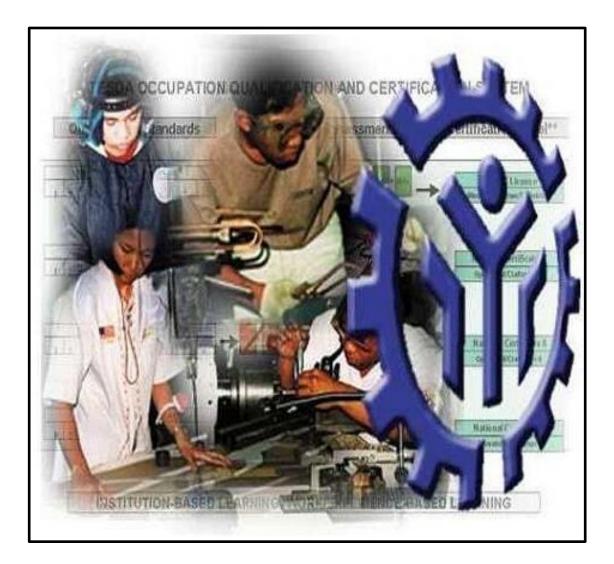# COMPETENCY STANDARDS

DATA PRIVACY AND ETHICS

INFORMATION AND COMMUNICATIONS TECHNOLOGY SECTOR

TECHNICAL EDUCATION AND SKILLS DEVELOPMENT AUTHORITY
East Service Road, South Luzon Expressway (SLEX), Taguig City, Metro Manila

Technical Education and Skills Development Act of 1994
(Republic Act No. 7796)

Section 22, "Establishment and Administration of the National Trade Skills Standards" of the RA 7796 known as the TESDA Act mandates TESDA to establish national occupational skills standards. The Authority shall develop and implement a certification and accreditation program in which private industry group and trade associations are accredited to conduct approved trade tests, and the local government units to promote such trade testing activities in their respective areas in accordance with the guidelines to be set by the Authority.

The Competency Standards (CS) serve as basis for the:

1. Competency-Based Curriculum;
2. Micro-Credential; and
3. Institutional Assessment Instruments

Each CS has two sections:

Section 1   **Definition of Qualification** describes the qualification and defines the competencies that comprise the qualification.

Section 2   **Competency Standards** gives the specifications of competencies required for effective work performance.

TABLE OF CONTENTS

ICT SECTOR

DATA PRIVACY AND ETHICS

COMPETENCY STANDARDS FOR
DATA PRIVACY AND ETHICS

SECTION 1: DEFINITION OF QUALIFICATION

The micro-competencies of DATA PRIVACY AND ETHICS provide the basic knowledge and skills to comply with privacy regulations and uphold ethical standards in data handling and processing.

The micro-competencies comprising Data Privacy and Ethics is:

UNIT CODE	**CORE COMPETENCIES**
CS-ICT251122	Ensure compliance with data privacy and ethics

SECTION 2:   COMPETENCY STANDARDS

This section gives the details of the contents of the units of competency required in **DATA PRIVACY AND ETHICS.**

CORE COMPETENCIES

UNIT OF COMPETENCY: ENSURE COMPLIANCE WITH DATA PRIVACY AND ETHICS

UNIT CODE: CS-ICT252101

UNIT DESCRIPTOR: This unit covers the outcomes required to ensure data privacy, ethical handling, and the integrity of data throughout its lifecycle. It includes maintaining compliance with data privacy regulations, applying ethical guidelines, and implementing practices to safeguard data accuracy and reliability across various projects.

ELEMENT	PERFORMANCE CRITERIA *Italicized terms* are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Comply with data privacy regulations	1.1. ***Data privacy regulations*** relevant to data handling are identified and followed based on industry standards 1.2. Data handling practices are ensured with Data privacy regulations 1.3. Secure storage practices are implemented to protect personal data based on industry standards	1.1. RA 10173 (Data Privacy Act of 2012). 1.2. Secure data storage protocols, including encryption and access control 1.3 Data Privacy Regulations	1.1. Identifying applicable data privacy regulations during annotation and labeling. 1.2. Following secure data handling procedures 1.3. Storing personal data in compliance with privacy laws
2. Apply ethical standards in data handling	2.1. ***Ethical guidelines*** are applied to avoid bias and promote fairness in data handling processes 2.2. Transparency in	2.1. Knowledge of AI ethics principles, such as fairness, transparency, and accountability	2.1. Applying ethical standards during annotation and labeling to avoid bias

| | data usage is ensured through proper documentation of **data handling practices**. | 2.2. RA 10175 (Cybercrime Prevention Act of 2012) | 2.2. Documenting data handling and usage practices |
| | 2.3. Consent for data usage is obtained and documented following **ethical standards** | 2.3. Importance of preventing bias in datasets and ensuring transparent practices | 2.3. Obtaining and recording user consent for data usage |

RANGE OF VARIABLES

VARIABLE	RANGE
1. Data privacy regulations	May include but not limited to: 1.1. RA 10173 (Data Privacy Act of 2012) 1.2. Organizational policies on data privacy
2. Ethical guidelines	May include but not limited to: 2.1. Guidelines to prevent bias in data annotation 2.2. Ethical AI principles 2.3. Transparency and accountability standards
3. Data handling practices	May include but not limited to: 3.1. Secure data transmission 3.2. Data anonymization 3.3. Data encryption
4. Ethical standards	May include but not limited to: 4.1. Fairness 4.2. Avoiding bias 4.3. Transparency 4.4. Accountability

EVIDENCE GUIDE

1. Critical aspects of competency	**Assessment requires evidence that the candidate:** 1.1 Complied with data privacy regulations 1.2 Applied ethical standards in data handling
2. Method of assessment	**The assessor may select from the following assessment methods but not limited to:** 2.1 Observation 2.2 Questioning 2.3 Practical demonstration
3. Resource implication	3.1 Access to relevant privacy regulations and ethical guidelines. 3.2 Documentation tools for compliance and tracking consent. 3.3 AI datasets requiring secure handling and compliance with privacy laws
4. Context of Assessment	4.1 Assessment may be conducted in a workplace or simulated environment.

GLOSSARY OF TERMS

Accuracy	The degree to which data or labels are correct and free from errors.
Annotation	The process of adding labels, tags, or metadata to data such as text, images, audio, or video to make it useful for machine learning.
Anonymization	A data privacy practice where personal identifiers are removed to protect individual identities.
Bias	Systematic error or unfair representation in data or labeling that can affect the performance of AI models. Examples include stereotypes or unbalanced datasets.
Completeness	A data quality metric that ensures all necessary data points are present and available.
Consistency	Ensuring data values follow the same format and standard throughout the dataset.
Data Ethics	Principles ensuring that data is collected, used, and shared in a way that is fair, transparent, and respects individual rights.
Data Privacy	The protection of personal information from unauthorized access or misuse.
Data Quality	A measure of the condition of data, ensuring it is accurate, complete, consistent, and timely.
Encryption	A method of securing data by encoding it so that only authorized parties can access it.
Fairness	Ensuring that AI models and datasets do not promote bias or discrimination.
RA 10173 (Data Privacy Act of 2012)	A Philippine law ensuring the protection of personal data by regulating its collection, processing, and storage.
RA 10175 (Cybercrime Prevention Act of 2012)	A Philippine law addressing legal issues related to online activities, including unauthorized access, data breaches, and identity theft.
RA 8293 (Intellectual Property Code of the Philippines)	A law that protects intellectual property rights, including copyrights, patents, and trademarks.
Transparency	Ensuring that processes and practices, such as data labeling, are clear and openly communicated to stakeholders.

ACKNOWLEDGEMENTS

Competency Standards are available in electronic copies, for more information, please contact:
Technical Education and Skills Development Authority (TESDA)
Tele Fax No.: 8818-7728
or visit our website: www.tesda.gov.ph