DATA PRIVACY MANUAL

Board Resolution No. 101
Series of 2025

WMSU-DPO-MN-001.00
Effective Date: 10-October-2025

DATA PRIVACY MANUAL
FOREWORD

The protection of personal data is not only a legal requirement but also a moral responsibility entrusted to us as an academic institution. In keeping with the provisions of the Data Privacy Act of 2012 (RA 10173), Western Mindanao State University affirms its unwavering commitment to safeguarding the personal information of our students, faculty, staff, and stakeholders.

This Institutional Data Privacy Manual has been developed to serve as the University's official guide in upholding the highest standards of lawful, transparent, and accountable practices in the collection, use, storage, sharing, retention, and disposal of personal data. It likewise outlines the responsibilities of all offices and personnel in protecting data privacy while supporting WMSU's mission in education, research, extension, and public service.

Beyond compliance, this Manual reflects the University's dedication to cultivating a culture of integrity and responsibility in the digital age. By prioritizing data protection, we ensure that our academic community and partners can place their trust in WMSU as an institution that values ethical governance and safeguards the rights of every individual.

May this Manual serve not only as a framework for compliance but also as a beacon of leadership, guiding us toward a future where respect for privacy and accountability remain at the heart of our University's pursuit of excellence.

DR. MA. CARLA A. OCHOTORENA
University President

TABLE OF CONTENTS

CHAPTER 1: BACKGROUND

Western Mindanao State University (WMSU) recognizes the vital importance of safeguarding personal information in accordance with Republic Act No. 10173, known as the **Data Privacy Act of 2012** (DPA). This legislation embodies the Philippine government's commitment to protecting the fundamental human right of privacy and ensuring secure communication in both government and private sectors. As an academic institution, WMSU acknowledges its responsibility to uphold these principles and ensure that personal data is handled with the utmost care and security.

The Data Privacy Act of 2012

The Data Privacy Act of 2012 was enacted to protect personal information in information and communications systems across the Philippines. It established the **National Privacy Commission (NPC)**, which is tasked with overseeing the law's implementation and ensuring compliance with data protection standards.

The primary objectives of the DPA include:

1. **Protecting Privacy:** Safeguarding the privacy of individuals while promoting the free flow of information to foster innovation and growth.
2. **Regulating Data Processing:** Governing the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of personal data.
3. **Ensuring Compliance with International Standards:** Aligning the Philippines with global data protection norms and standards through the NPC's guidance.

Under the DPA, organizations processing personal data, known as Personal Information Controllers (PICs) or Personal Information Processors (PIPs), are required to implement reasonable and appropriate measures to protect personal data from both natural and human threats. These threats include accidental loss, destruction, unlawful access, fraudulent misuse, alteration, and contamination.

CHAPTER 2: INTRODUCTION

Western Mindanao State University (WMSU) recognizes the right to privacy as a fundamental human right that must be safeguarded, especially in the modern digital age, where information is easily shared and accessed. The protection of personal information is not only a legal obligation but also a moral imperative for any institution that handles personal data.

As a leading academic institution, WMSU is dedicated to ensuring the privacy and security of personal information entrusted to it by students, faculty, staff, alumni, and other stakeholders. This commitment extends to all facets of its operations, including academic, administrative, and research and extension activities. By implementing robust privacy practices, the University aims to create a secure environment where personal data is handled with the utmost care and responsibility.

In line with this commitment, WMSU has adopted this Privacy Manual to articulate its dedication to upholding data privacy rights and to serve as a guide for the University's data protection practices. This manual outlines the principles, policies, and procedures that govern the collection, use, storage, and disposal of personal information within WMSU's information and communications systems. It is designed to ensure that all university activities involving personal data comply with the Data Privacy Act of 2012 (Republic Act No. 10173), its Implementing Rules and Regulations (IRR), and the relevant issuances of the National Privacy Commission (NPC).

CHAPTER 3: DEFINITION OF TERMS

Anonymization. The process of removing or modifying personal identifiers from a dataset so that an individual can no longer be reasonably and directly identified. Proper anonymization places the dataset outside the scope of “personal information” under the Data Privacy Act of 2012.

Consent of the Data Subject. Any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to them. Consent shall be evidenced by written, electronic, or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

Compliance Officer for Privacy (COP). An official or personnel designated within a specific unit, college, or office of Western Mindanao State University to assist the Data Protection Officer (DPO) in ensuring compliance with the Data Privacy Act of 2012, its IRR, and issuances of the National Privacy Commission.

Data Privacy Committee. The Data Privacy Committee is a body designated to assist the Data Protection Officer (DPO) in implementing and monitoring the University's compliance with the Data Privacy Act of 2012. It supports the development of privacy policies, promotes data protection awareness, and helps manage privacy risks across the institution.

Data Protection Officer (DPO). The official of Western Mindanao State University tasked with independent and autonomous jurisdiction and authority over data protection and privacy matters. The DPO monitors compliance with the Data Privacy Act, its Implementing Rules and Regulations (IRR), issuances by the National Privacy Commission (NPC), and other applicable laws and policies.

Data Sharing. The disclosure or transfer of personal data under the custody of a Personal Information Controller or Personal Information Processor to a third party. In the case of the latter, such disclosure or transfer must have been upon the instructions of the Personal Information Controller concerned. Data sharing excludes outsourcing or the disclosure or transfer of personal data by a Personal Information Controller to a Personal Information Processor.

Data Subject. An individual whose personal, sensitive personal, or privileged information is processed by Western Mindanao State University. It may refer to officers, employees, consultants, students, parents, guardians, faculty, visiting faculty, staff, researchers, research subjects, patients, clients, customers, alumni, donors, applicants, and other stakeholders.

Electronic Signature (E-Signature). Refers to any distinctive electronic symbol, mark, or process attached to, or logically associated with, an electronic document and executed or adopted by a person with the intent to sign, authenticate, or approve the document, in accordance with Republic Act No. 8792 (E-Commerce Act of 2000) and the Rules on Electronic Evidence.

Personal Data. All types of personal information, sensitive personal information, or privileged information as defined by the Data Privacy Act of 2012 or any subsequent law.

Personal Data Breach. 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.

Personal Information. 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 information, or when put together with other information, would directly and certainly identify an individual.

Personal Information Controller (PIC). An official or personnel who controls the collection, holding, processing, use, transfer, or disclosure of personal information, including an official/personnel who instructs another official/personnel to collect, hold, process, use, transfer, or disclose personal information on their behalf. There is control if the official/personnel decides on what information is collected, or the purpose or extent of its processing. The term excludes an official/personnel who performs such functions as instructed by another official/personnel, and an official/personnel who collects, holds, processes, uses, transfers, or discloses personal information in connection with the individual's personal, family, or household affairs**.** In Western Mindanao State University (WMSU), the University itself, represented by the University President, is the Personal Information Controller (PIC).

Personal Information Processor (PIP). Any natural or juridical person qualified to act as such under the Data Privacy Act and its Implementing Rules and Regulations to whom a Personal Information Controller may outsource or instruct the processing of personal data pertaining to a data subject.

Privileged Information. Any and all forms of data that, under the Rules of Court and other pertinent laws, constitute privileged communication.

Processing. Any operation or set of operations performed upon personal information, including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.

Sensitive Personal Information (SPI). Personal information that includes:

- About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations.
- About an individual's health, education, genetic or sexual life, or any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings.
- 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.
- Specifically established by an executive order or an act of Congress to be kept classified.

CHAPTER 4: SCOPE AND LIMITATIONS

Section 4.1: Scope

This Privacy Manual applies to the processing of all types of personal information handled by Western Mindanao State University. It governs the acts and decisions of the following:

a. All types of students, parents, guardians, faculty, visiting faculty, admin personnel and staff.
b. Research, Extension, and Professional Staff (REPS).
c. WMSU contractual personnel, Non-WMSU contractual personnel, and retirees.
d. Applicant students, applicant faculty, and applicant staff.
e. Researchers, research subjects, extensionists, beneficiaries, extension stakeholders, patients, clients, and customers.
f. Alumni, donors, donees, contract counterparties, partners, subcontractors, suppliers, licensors, and licensees.

All personnel of the University, regardless of the type of employment or contractual arrangement, including regular, contractual, or project-based employees, must comply with the terms set out in this Manual. The provisions of this Manual shall take effect upon approval by the University Board of Regents and shall remain in force until amended or revoked by the Board of Regents, upon the recommendation of the Data Protection Officer (DPO)

Section 4.2: Limitations

This Manual does not apply to the following situations and information:

a. Government Officials and Employees

Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

a.1. The fact that the individual is or was an officer or employee of the government institution.
a.2. The title, business address, and office telephone number of the individual.
a.3. The classification, salary range, and responsibilities of the position held by the individual.
a.4. The name of the individual on a document prepared by the individual in the course of employment with the government.

b. Contractual Services

Information about an individual who is or was performing service under contract for a government institution, but only insofar as it relates to such service, including the name of the individual and the terms of their contract.

c. Financial Benefits

Information relating to a benefit of a financial nature conferred on an individual upon the discretion of the government, such as the granting of a license or permit, including the name of the individual and the exact nature of the benefit. This exclusion does not cover benefits given in the course of an ordinary transaction or as a matter of right.

d. Journalistic, Artistic, or Literary Purposes

Personal information processed for journalistic, artistic, or literary purposes to uphold freedom of speech, expression, or the press, subject to the requirements of other applicable laws or regulations.

e. Research and Extension Purposes

Personal information processed for research and extension purposes intended for public benefit, subject to the requirements of applicable laws, regulations, or ethical standards.

f. Public Authority Functions

Information necessary to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function. This includes the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law.

g. Banking and Financial Information

Information necessary for banks, other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas (BSP), and other bodies authorized by law, to the extent necessary to comply with Republic Act No. 9510 (Credit Information System Act), Republic Act No. 9160, as amended (Anti-Money Laundering Act), and other applicable laws.

h. Foreign Jurisdictions

Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines. The burden of proving the law of the foreign jurisdiction falls on the person or body seeking exemption. In the absence of proof, the applicable law shall be presumed to be the Data Privacy Act (DPA) and its Implementing Rules and Regulations (IRR).

Compliance and Interpretation:

a. The non-applicability of this Manual does not extend to Personal Information Controllers (PIC) or Personal Information Processors (PIP), who remain subject to the requirements of implementing security measures for personal data protection.
b. The processing of the information provided in the preceding sections shall be exempted from the requirements of this M anual only to the minimum extent necessary to achieve the specific purpose, function, or activity.
c. Unless directly incompatible or inconsistent with the preceding sections in relation to the purpose, function, or activities, the PIC or PIP shall uphold the rights of data subjects and adhere to general data privacy principles and the requirements of lawful processing.
d. The burden of proving that this Manual is not applicable to a particular information falls on those involved in the processing of personal data or the party claiming the non-applicability.
e. In all cases, the determination of any exemption shall be liberally interpreted in favor of the rights and interests of the data subject.

CHAPTER 5: DATA PRIVACY PRINCIPLES

In all actions and decisions involving personal data, Western Mindanao State University (WMSU) shall ensure that the following privacy principles are applied in accordance with the Data Privacy Act of 2012 and other applicable laws:

Section 5.1: Principles of Transparency, Legitimate Purpose, and Proportionality

a. Transparency

Awareness: The data subject must be aware of the nature, purpose, and extent of the processing of their personal data, including the risks and safeguards involved, the identity of the Personal Information Controller (PIC), their rights as a data subject, and how these can be exercised.

Communication: Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

b. Legitimate Purpose

Purpose Alignment: The processing of information shall be compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy.

c. Proportionality

Relevance: The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

Efficiency: Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Section 5.2: General Principles for Collection, Processing, and Retention of Personal Data

The processing of personal data at WMSU shall adhere to the following general principles:

a. Collection for a Declared Purpose

Lawful Basis: Personal data shall be collected and processed only when there is a valid legal basis under the Data Privacy Act of 2012 (RA 10173), such as:

a.1. Compliance with laws and regulations applicable to WMSU as a public higher education institution (e.g., CSC, COA, CHED, NAP rules);

a.2. Performance of a public authority function vested in WMSU by RA 8292 and related issuances;

a.3. Consent of the data subject, when no other lawful basis applies;

a.4. Other grounds permitted under Sections 12 and 13 of RA 10173.

Consent: When processing is based on consent, it must be freely given, informed, and time-bound with respect to the declared, specified, and legitimate purpose. Consent may be withdrawn at any time without retroactive effect on prior lawful processing.

Transparency: Data subjects must be provided with specific information regarding the purpose and extent of processing, including, where applicable, automated processing, profiling, or data sharing.

Necessity: Only personal data that is necessary and compatible with the declared, specified, and legitimate purpose shall be collected.

b. Fair and Lawful Processing

Rights: Processing shall uphold the rights of the data subject, including the right to refuse, withdraw consent, or object. It shall likewise be transparent and allow the data subject sufficient information to know the nature and extent of processing.

Clarity: Information provided to a data subject must always be in clear and plain language to ensure that it is easy to understand and access.

Purpose Compatibility: Processing must be in a manner compatible with the declared, specified, and legitimate purpose.

Adequacy: Processed personal data should be adequate, relevant, and limited to what is necessary concerning the purposes for which they are processed.

Safeguards: Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.

c. Data Quality

Accuracy: Personal data should be accurate and, where necessary for the declared, specified, and legitimate purpose, kept up to date.

Rectification: Inaccurate or incomplete data must be rectified, supplemented, destroyed, or their further processing restricted.

d. Retention and Disposal

Retention Period: Personal data shall be retained only as long as necessary for its declared purpose or as required under the records retention schedules of the **National Archives of the Philippines (NAP)**.

Legal and Administrative Needs: Data may be kept to comply with laws, regulatory requirements, audits, or legal claims, consistent with standards of COA, CSC, CHED, NAP, and other government agencies.

Academic and Alumni Records: Certain records—such as student transcripts, diplomas, and academic credentials—shall be retained permanently to serve alumni needs and institutional archiving, subject to NAP guidelines and secure access controls.

Archival Value: Long-term retention is allowed when necessary for institutional archiving, historical preservation, or compliance with NAP-approved schedules.

Secure Disposal: Records whose retention periods have lapsed shall be disposed of securely, in accordance with NAP rules, ensuring they cannot be reconstructed, accessed, or misused.

e. Further Processing and Data Sharing

Authorized Processing: Any authorized further processing shall have adequate safeguards. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes. In cases laid down in law, they may be stored for longer periods, subject to implementing the appropriate organizational, physical, and technical security measures required by the Data Privacy Act to safeguard the rights and freedoms of the data subject.

Anonymized Data: Personal data that is aggregated or kept in a form that does not permit the identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.

Prohibited Retention: Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

Section 5.3: General Principles for Data Sharing

WMSU acknowledges the importance of collaboration with external entities—such as government agencies, research institutions, and development partners—for advancing knowledge, innovation, extension activities, and public service. The further processing or sharing of personal data collected by the University from a party other than the data subject shall be allowed only under the following conditions:

a. Legal Authorization

Lawful Sharing: Data sharing is permitted when expressly authorized by law or regulation, provided that appropriate safeguards for privacy and security are in place.

Principles: All processing must adhere to the principles of transparency, legitimate purpose, and proportionality as mandated by the Data Privacy Act of 2012 (RA 10173).

b. Research, Academic, and Extension Collaboration

With Consent or Public Data: Personal data collected from parties other than the data subject for research and extension purposes may be shared when:

The data subject has given explicit, informed consent; or

The data is already publicly available and its use does not violate any ethical or legal restrictions.

Protection of Rights: The privacy rights of data subjects shall be upheld at all times. No decision that directly affects the individual shall be made solely on the basis of this shared data, without appropriate validation or safeguards.

Safeguards: When external entities (e.g., DOST, CHED, LGUs) request data from university-led research or extension activities, such sharing shall:

b.1. Be governed by a Data Sharing Agreement (DSA) or Memorandum of Agreement (MOA) that outlines scope, purpose, data classification, security measures, retention, and accountability.

b.2. Undergo a Privacy Impact Assessment (PIA), if applicable, especially when sharing involves sensitive or large-scale data.

c. Inter-Agency Government Data Sharing

Public Function and Service: Sharing of personal data between WMSU and other government agencies (e.g., DOST, CHED, DICT) for the purpose of performing a public function, conducting official research, or delivering public service shall:

c.1. Be covered by a formal Data Sharing Agreement (DSA);

c.2. Include provisions that ensure data minimization, security controls, data subject rights, and purpose limitation;

c.3. Be reviewed by the WMSU Data Protection Officer (DPO) to ensure consistency with data protection obligations.

CHAPTER 6. PROCESSING OF PERSONAL DATA

Western Mindanao State University (WMSU) processes personal data in line with its role as a higher education institution, research body, and government entity. This section outlines the lawful grounds, purposes, and classifications of personal data processed by WMSU, as well as the protocols for ensuring data privacy and security.

Section 6.1: Grounds and Purposes of Processing Personal Data

WMSU processes personal data based on several legitimate grounds, each tied to the university's responsibilities and objectives. These grounds ensure that any processing activity is conducted legally and ethically:

a. Performance of Obligations and Exercise of Rights:

Government Instrumentality: As an institution that serves public functions, WMSU processes personal data to fulfill its duties as an extension of the government. This includes providing educational services, conducting research, and maintaining public safety and welfare.

Higher Education Institution: WMSU processes data to deliver educational programs, evaluate academic performance, and provide student support services. This involves managing student records, faculty evaluations, and administrative tasks to ensure quality education.

b. Pursuance of Institutional Mandates:

Under Legal Mandates: WMSU operates under legal frameworks and mandates, such as its charter and government directives, which require processing personal data to meet educational and research objectives.

University-Specific Functions: Each department within WMSU may process personal data to perform tasks that are typical and necessary for similar academic and administrative bodies, ensuring smooth operations and effective governance.

c. Student and Community Welfare:

Holistic Support: WMSU prioritizes the well-being of its students, parents, guardians, faculty, staff, researchers, alumni, and the broader community. This involves processing data to provide comprehensive support services, including counseling, academic advising, and community outreach programs.

d. Internal and External Management:

Academic and Research Institution: WMSU processes personal data to manage its internal affairs, such as admissions, human resources, and academic evaluations, while also engaging in external collaborations and partnerships that enhance educational and research opportunities.

WMSU processes personal data for the following purposes:

a. Academic, Research and Extension Activities

To facilitate learning, teaching, and research initiatives, WMSU collects and analyzes personal data related to student performance, research participation, and faculty development. All

processing shall be conducted lawfully, ensuring that research ethics, academic freedom, and the rights of data subjects are respected at all times. Safeguards will be applied to protect sensitive research data and ensure its use strictly aligns with declared academic and scientific purposes.

In situations where researchers request access to personal or sensitive information, WMSU may allow the release of data provided that appropriate safeguards, such as **anonymization** or **pseudonymization**, are applied. Anonymization involves removing or modifying personal identifiers (e.g., names, student IDs, addresses, or other unique attributes) so that individuals can no longer be reasonably and directly identified. Once properly anonymized, such datasets are no longer considered "personal information" under the Data Privacy Act of 2012.

The following conditions shall apply to research data requests involving anonymization:

a.1. Requests must undergo review and approval by the Data Protection Officer (DPO), in consultation with the relevant academic or administrative units.
a.2. Data Sharing Agreements (DSA) or similar instruments shall be executed, setting clear terms on purpose, scope, safeguards, and limitations of use.
a.3. An audit trail of the anonymization process must be documented, including who performed the anonymization and the methods applied.
a.4. Researchers shall only receive the minimum necessary data to achieve the declared academic or scientific purpose.
a.5. Re-identification or unauthorized use of anonymized data is strictly prohibited and will be subject to disciplinary and legal consequences.

b. Student and Employee Welfare

Personal data is used to provide support services such as healthcare, counseling, career guidance, and financial aid, ensuring the well-being and success of students and staff. The University commits to treating such welfare-related data with utmost confidentiality, applying medical and psychological data protection standards, and limiting access only to duly authorized personnel to prevent stigmatization, discrimination, or misuse.

c. Administrative Management

WMSU processes data for administrative functions, including admissions, enrollment, employment, payroll, and facility management, ensuring efficient and effective operations. All administrative data processing shall follow lawful protocols, applying strict verification, access control, and recordkeeping procedures to maintain integrity, transparency, and accountability in governance.

d. Legal and Regulatory Compliance

The University processes personal data to comply with legal obligations, regulatory requirements, and government reporting mandates, ensuring accountability and transparency. In doing so, WMSU shall exercise due diligence in collecting only data that is lawfully required, disclosing information only to authorized government agencies, and maintaining documentation of compliance activities for audit and oversight purposes.

e. Community Engagement and Partnerships

WMSU engages with alumni, donors, and external partners to build relationships and secure funding, necessitating the processing of relevant personal data. The University shall process and share such data only with consent or proper legal basis, ensuring transparency, adherence to data sharing agreements, and protection of the rights and interests of all stakeholders.

f. Safety and Security

Personal data is processed to ensure campus safety, manage emergency responses, and uphold security measures, safeguarding the WMSU community and its facilities. The University commits to carefully balancing the need for safety with respect for individual rights, ensuring that surveillance, monitoring, or incident reporting mechanisms are proportional, justified, and equipped with adequate safeguards against misuse.

g. Quality Assurance and Evaluation

WMSU uses personal data to assess the quality of its programs, services, and faculty, implementing improvements based on feedback and evaluations to enhance the overall educational experience. All evaluation and feedback data shall be processed in a fair, lawful, and transparent manner, anonymizing or pseudonymizing responses whenever applicable to protect the identity of individuals and encourage open, honest participation.

h. Financial Management

Processing personal data for financial transactions, budgeting, and auditing purposes is essential for maintaining WMSU's financial health and sustainability. The University shall ensure that all activities involving financial data are carried out with extensive, careful, and lawful procedures in strict compliance with the Data Privacy Act of 2012, its Implementing Rules and Regulations, and relevant issuances of the National Privacy Commission. This includes implementing adequate safeguards to protect sensitive financial information, limiting access only to authorized personnel, and adopting accountability mechanisms to prevent misuse, fraud, or unauthorized disclosure.

i. Marketing and Service Delivery

Personal data may be processed for purposes related to marketing and service delivery in connection with WMSU's institutional activities, such as alumni engagement, income-generating projects, and public service initiatives. Processing for these purposes shall:

i.1. Be covered by appropriate privacy notices and, where applicable, consent from the data subject.
i.2. Be limited to the minimum necessary data required for the declared activity.
i.3. Not involve unauthorized disclosure or use beyond the declared scope.
i.4. Respect the rights of data subjects to object to marketing-related processing of their data."

j. Income-Generating Projects

WMSU processes personal data for the effective management of its income-generating projects (IGPs), which may include:

j.1. Customer Data (e.g., client records for training programs, short courses, and facility rentals)
j.2. Employee Data (e.g., records of contractual employees directly engaged in IGP operations)
j.3. Supplier and Partner Data (e.g., contact details, contract terms, and transaction records)

Processing of such data shall comply with the principles of transparency, legitimate purpose, and proportionality, ensuring that only the minimum necessary data is used and safeguarded."

Specific privacy notices may be provided for initiatives that involve data processing, detailing how personal data will be used and protected.

Section 6.2: Types of Personal Data Processed

WMSU processes a variety of personal data types to fulfill its academic, administrative, research and extension functions. This data is collected, stored, and utilized in compliance with applicable laws and regulations:

a. Personal Details

Includes name, date of birth, gender, civil status, and affiliations. This information is crucial for identity verification, enrollment, and record-keeping.

b. Contact Information

Encompasses home address, email, phone numbers, and emergency contacts. WMSU uses this data to communicate with students, staff, and stakeholders effectively.

c. Academic Information

Covers grades, courses, academic standing, and performance metrics. This data supports student evaluations, degree progress assessments, and academic advising.

d. Employment Information

Involves government-issued IDs, job titles, roles, and employment history. It is essential for managing staff records, payroll, and HR functions.

e. Applicant Information

Comprises educational background, previous employment, and references. This information is used in admissions and hiring processes to evaluate eligibility and suitability.

e. Medical Information

Includes health records, medical history, and test results. This sensitive data is handled with strict confidentiality to provide medical care and support to students and staff.

f. Financial Information

Consists of banking details, tuition payments, and financial aid data. WMSU processes this information to manage financial transactions and student accounts.

h. Behavioral and Disciplinary Information

Pertains to conduct, disciplinary actions, and incident reports. This data is used to maintain campus safety and uphold university standards.

i. Alumni Information

Encompasses contact details, employment status, and involvement in alumni activities. This data facilitates alumni engagement, networking, and fundraising efforts.

j. Images and Videos

Includes photographs, CCTV footage, and recorded events. This media is used for security, marketing, and documentation purposes, adhering to privacy guidelines.

k. Biometric Data

Includes fingerprints, facial scans, iris patterns, or other biometric identifiers used for identity verification, attendance monitoring, or access control. Biometric data is classified as Sensitive Personal Information under the Data Privacy Act of 2012.

Section 6.3: Data Classification

Personal data at WMSU is categorized based on sensitivity and access requirements, ensuring appropriate protection and handling:

a. Public Data

Information that is freely accessible to the public, such as course catalogs, event announcements, and general university information. Public data is not subject to restrictions but is still managed responsibly to ensure accuracy and reliability.

b. Internal Data

Data intended for use within specific WMSU units or departments. Access is restricted to authorized personnel who require the information to perform their duties. Examples include internal memos, departmental reports, and non-sensitive employee records. *Risk level is Low.* Internal data poses minimal risk to WMSU if disclosed, but unauthorized access could result in reputational damage or operational disruptions.

c. Confidential Data

Information that should only be disclosed to a limited group of individuals to protect WMSU from legal, financial, or reputational risks. Examples include personal information like home addresses, academic records, and employee evaluations. *Risk Level is Medium.* Confidential data poses a moderate risk, and unauthorized access could lead to legal liabilities or violations of individual privacy rights.

d. Sensitive Confidential Data

Highly sensitive information that could cause significant harm to WMSU or individuals if disclosed. This category includes sensitive personal data, such as health records, political affiliations, and legal case details. *Risk level is High.* Sensitive confidential data requires the highest level of protection, with access limited to only those who absolutely need it for critical purposes.

Data Restrictions

WMSU employs data restrictions to safeguard information, assigning access levels based on the risk and sensitivity of the data:

a. Internal Data Restrictions:

Definition: Data that should remain within specific units or offices for internal use only.

Access: Authorized personnel within the relevant WMSU units who need the data for their responsibilities.

Examples: Employee benefits accessible by HR and Accounting, draft documents not yet approved for public release.

b. Confidential Data Restrictions:

Definition: Data that requires restricted access to prevent legal, financial, or reputational risks.
Access: Authorized WMSU officials, staff, or faculty members with a legitimate need for the data.
Examples: Personal information such as home addresses, email addresses, and intellectual property like patent applications.

c. Sensitive Confidential Data Restrictions:

Definition: Data that poses a high risk and requires strict protection.
Access: Limited to a minimum number of authorized individuals with a critical need to know.
Examples: Sensitive personal information such as age, political affiliation, health records, and privileged information related to legal cases.

Public Data

Public data is openly accessible to both internal and external parties and is subject to minimal restrictions. However, WMSU ensures that even public data is accurate and used appropriately:
Definition: Data that can be accessed by the public without restrictions, such as university publications, research findings, and general information.
Access: Freely available to anyone, both within and outside WMSU.
Examples: University announcements, press releases, and course information.

Requests for public data must comply with the WMSU Freedom of Information Manual, ensuring transparency and accountability in data sharing.

Section 6.4: Processing of Biometric Data for Attendance Monitoring

In recognition of the legitimate institutional interest in modernizing attendance monitoring systems while upholding data privacy and academic freedom, Western Mindanao State University (WMSU) shall process biometric data of faculty and staff for Daily Time Record (DTR) purposes only, in accordance with the Data Privacy Act of 2012 (R.A. 10173)**,** the Administrative Code of 1987**,** Civil Service Commission (CSC) rules on attendance**,** Commission on Audit (COA) internal control regulations**,** and R.A. 8292 (Higher Education Modernization Act of 1997)**.**

a. Enabling Policy Requirement

a.1. The biometric attendance system shall be implemented pursuant to a formally approved institutional policy, including a Board of Regents resolution under R.A. 8292, which shall expressly:
a.2. Affirm the necessity of the biometric system to comply with CSC Memorandum Circular No. 21, s. 1991 and related issuances on daily attendance recording, consistent with Book V, Title I, Subtitle A, Chapter 6, Sec. 46(b)(8) of the Administrative Code of 1987 on attendance accountability of government personnel;
a.3. Recognize its role in payroll validation, prevention of irregularities, and compliance with COA regulations on internal control and audit trails;
a.4. Sections 12(c) and 12(e) of the Data Privacy Act, which allow processing of personal data where necessary for compliance with a legal obligation or for the performance of public authority functions, thereby establishing that consent is not required;
a.5. Provide for appropriate privacy and security safeguards to ensure lawful, fair, and transparent processing of biometric data.

b. Conduct of a Privacy Impact Assessment (PIA)

Prior to system roll-out, WMSU shall conduct a thorough Privacy Impact Assessment (PIA) in accordance with NPC Advisory Guidelines, to identify risks and recommend safeguards.
The PIA shall cover:

b.1. The type and scope of biometric data collected, which qualifies as sensitive personal information under Sec. 3(l) of R.A. 10173**;**
b.2. The storage, retention, and disposal period, ensuring compliance with the data minimization principle under Sec. 11 of R.A. 10173;
b.3. Access control and user authentication protocols consistent with the principles of confidentiality, integrity, and availability (CIA Triad) under information security standards.

c. Sensitive Personal Data Safeguards
Since biometric data is classified as sensitive personal information under R.A. 10173, Sec. 13, WMSU commits to:
Encrypt all biometric data during storage and transmission, in compliance with the NPC Circular on Security of Personal Data;

c.1. Limit access strictly to authorized personnel, following the **"**need-to-know" principle under Sec. 20 of R.A. 10173;
c.2. Prohibit any secondary or unauthorized use of biometric data, ensuring alignment with Sec. 18 on data subject rights.

d. Stakeholder Orientation, Engagement and Academic Considerations
WMSU shall conduct consultations with duly recognized employee unions and stakeholders before adoption of the biometric policy. Special consideration shall be provided to:

d.1. Faculty members with fieldwork, research, hospital, or court-related responsibilities whose work arrangements may require alternative attendance validation;
d.2. Ensuring proportionality of measures, so that biometric use enhances accountability while respecting individual rights.

Section 6.5: Processing of E-Signatures

a. Purpose and Scope
The University may allow the use of electronic signatures (e-signatures) in official transactions, such as:

a.1. Approvals of internal memoranda, office communications, and academic documents;
a.2. Student and employee requests processed through digital platforms;
a.3. Human resource, financial, and procurement documents;
a.4. Contracts, Memoranda of Agreement (MOAs), and partnerships, subject to the approval of appropriate authorities and the Board of Regents.

b. Legal Recognition
E-signatures executed within the University's approved systems shall have the same legal effect as handwritten signatures, provided identity verification and authentication safeguards are in place.

c. Authentication and Integrity

c.1. The University shall adopt secure platforms ensuring authenticity, traceability, and tamper-resistance of e-signatures.
c.2. Authentication measures, such as official university accounts, one-time passwords, or equivalent controls, shall be implemented as applicable.
c.3. Metadata including signer identity, date, and time stamp shall form part of the audit trail of every e-signed document.

d. Data Privacy and Security

d.1. E-signatures are considered personal and sensitive personal information. Their processing shall adhere to the principles of transparency, legitimate purpose, and proportionality.
d.2. Access to e-signed records shall be restricted to authorized personnel only.
d.3. Retention and disposal of e-signed documents shall comply with the Records Disposition Schedule (RDS) approved by the National Archives of the Philippines (NAP).

e. Limitations
The use of e-signatures shall not extend to documents requiring "wet" signatures under existing laws, such as notarized documents, land titles, or Commission on Audit (COA) and Civil Service Commission (CSC) forms, unless expressly authorized by government issuances.

Section 6.5: Cross-Border Data Flow

WMSU acknowledges that certain academic, research, alumni, and resource generation initiatives may involve the transfer of personal data across national borders. Cross-border data transfers shall only be conducted under the following conditions:

a. Compliance with the Data Privacy Act of 2012 and applicable foreign data protection laws.

b. Existence of adequate safeguards, including data sharing agreements (DSA) or memoranda of understanding (MOU) with international partners.

c. Limiting the transfer to the minimum data necessary for the declared academic, research, or institutional purpose.

d. Ensuring that recipients of WMSU data uphold privacy standards consistent with Philippine laws and international norms."

CHAPTER 7: SECURITY MEASURES

Western Mindanao State University (WMSU) is dedicated to safeguarding personal information by implementing robust security measures that protect against both natural and human threats. These measures ensure the availability, integrity, and confidentiality of personal data, aligning with the principles of the Data Privacy Act of 2012. This commitment is vital for maintaining trust and compliance with legal and ethical standards in the academic environment.

Section 7.1: Organizational Security Measures

a. Designation of a Data Protection Officer (DPO)

In compliance with the Data Privacy Act of 2012, WMSU shall appoint a dedicated Data Protection Officer (DPO). The DPO is responsible for leading the university's data protection efforts and ensuring that all practices align with legal and ethical standards. Key responsibilities include:

a.1. **Monitoring Compliance:** Regularly assess and monitor the university's adherence to data privacy laws, including the Data Privacy Act, its Implementing Rules and Regulations (IRR), and other relevant policies. The DPO will ensure that WMSU's data handling practices are up-to-date and compliant with the latest legal requirements.

a.2. **Conducting Privacy Impact Assessments (PIA):** Perform Privacy Impact Assessments to evaluate potential risks associated with data processing activities, projects, and systems. This proactive approach identifies vulnerabilities and implements safeguards to protect personal information.

a.3. **Advising on Complaints and Rights:** Provide guidance on addressing data privacy complaints and assist data subjects in exercising their rights, such as access to information, correction, and erasure.

a.4. **Managing Data Breaches:** Establish protocols for managing data breaches and security incidents. The DPO will oversee the preparation and submission of reports to the National Privacy Commission (NPC) and ensure timely response to incidents.

a.5. **Promoting Awareness:** Cultivate a culture of privacy awareness within the university. This includes organizing training sessions and disseminating information about data protection laws, rules, and best practices.

a.6. **Policy Development:** Advocate for the development and revision of privacy policies and guidelines. The DPO will ensure a privacy-by-design approach, integrating data protection into all university operations and projects.

a.7. **Liaison with Authorities:** Serve as the main contact point for data subjects, the NPC, and other authorities on matters related to data privacy and security. The DPO will coordinate with external bodies to enhance compliance and resolve issues.

a.8. **Collaboration and Support:** Work closely with university units to support data privacy initiatives and provide expert advice on privacy-related matters. The DPO will lead efforts to integrate data privacy into the university's strategic goals.

b. Appointment of Compliance Officers for Privacy (COP)

Each unit within WMSU will appoint a Compliance Officer for Privacy (COP) to act as the local representative for data privacy matters. The COP will ensure that their respective unit adheres to data privacy principles and complies with university policies. Responsibilities include:

b.1. **Local Data Privacy Champion:** The COP will act as the primary advocate for data privacy within their unit, ensuring that all personnel understand and uphold privacy principles in their daily activities.
b.2. **Training and Education:** Facilitate training sessions and seminars to educate unit personnel on data privacy and security practices. The COP will tailor training to address the specific needs and risks of their unit.
b.3. **Incident Reporting:** Serve as the first point of contact for reporting data breaches and security incidents within the unit. The COP will work closely with the DPO to manage incidents and implement corrective measures.
b.4. **Compliance Monitoring:** Regularly review unit practices to ensure compliance with data privacy policies and procedures. The COP will identify areas for improvement and collaborate with the DPO to enhance data protection measures.
b.5. **Representation in Privacy Matters:** Represent their unit in official meetings and events related to data privacy. The COP will collaborate with other units to share best practices and coordinate university-wide privacy initiatives.

c. Training and Seminars

WMSU is committed to fostering a culture of data privacy awareness through regular training and seminars. These programs are designed to equip personnel with the knowledge and skills necessary to protect personal information effectively:

c.1. **Mandatory Annual Training:** All employees will participate in mandatory annual training sessions covering data privacy principles, legal obligations, and best practices. These sessions will be updated regularly to reflect changes in legislation and emerging threats.
c.2. **Targeted Training for Key Personnel:** Personnel directly involved in processing personal information, such as data handlers, IT staff, and administrative staff, will receive specialized training. This targeted approach ensures that those with the most access to personal data are well-prepared to handle it securely.
c.3. **Workshops and Seminars:** WMSU will organize workshops and seminars to address specific topics, such as data breach response, privacy impact assessments, and the ethical use of data. These events will be open to all university personnel and provide opportunities for interactive learning and discussion.
c.4. **Awareness Campaigns:** The university will conduct awareness campaigns to reinforce the importance of data privacy. These campaigns will include posters, newsletters, and digital content to keep data privacy at the forefront of daily operations.

d. Privacy Impact Assessments (PIA)

Privacy Impact Assessments (PIAs) are crucial for identifying and mitigating risks associated with personal information processing. WMSU will conduct PIAs for all relevant activities, projects, and systems:

d.1. **Risk Identification:** PIAs will systematically identify potential privacy risks associated with data processing activities. This process will involve evaluating the types of data collected, the purposes of processing, and potential impacts on data subjects.
d.2. **Mitigation Strategies:** Based on the PIA findings, the university will implement appropriate safeguards to mitigate identified risks. These strategies may include technical measures, policy adjustments, and process improvements.
d.3. **Collaboration with Process Owners:** The DPO will collaborate with process owners to develop PIA documents tailored to specific projects and systems. This collaborative approach ensures that all stakeholders are involved in the assessment process and that privacy considerations are integrated into decision-making.
d.4. **Ongoing Monitoring:** PIAs will be regularly reviewed and updated to reflect changes in processing activities, technologies, and legal requirements. This ongoing monitoring ensures that the university remains proactive in addressing privacy risks.

e. Data Privacy Review Team

WMSU will establish a Data Privacy Review Team responsible for overseeing and auditing the implementation of the university's data privacy policies:

e.1. **Leadership by the DPO:** The team will be led by the DPO, who will coordinate efforts to evaluate compliance across all university units. The team will work closely with unit heads to assess practices and identify areas for improvement.
e.2. **Comprehensive Audits:** The team will conduct comprehensive audits of data privacy practices, policies, and procedures. These audits will evaluate the effectiveness of security measures, data handling processes, and staff compliance with privacy guidelines.

e.3. **Detective Controls:** The team will employ a combination of process, human capital, physical, and technological controls to assess compliance. These controls will provide a holistic view of the university's data privacy landscape and identify potential vulnerabilities.

e.4. **Annual Reporting:** The team will produce annual reports detailing audit findings, recommendations, and progress on implementing data privacy initiatives. These reports will be shared with university leadership to support informed decision-making and strategic planning.

f. Non-Disclosure Agreements

To maintain confidentiality and protect sensitive information, all WMSU employees with access to personal data will be required to sign a Non-Disclosure Agreement (NDA):

f.1. **Confidentiality Obligations:** The NDA will outline employees' obligations to maintain the confidentiality of personal information and prohibit unauthorized disclosure or misuse of data.

f.2. **Enforcement and Compliance:** WMSU will enforce compliance with NDAs through regular monitoring and disciplinary measures for violations. This approach underscores the importance of confidentiality and promotes a culture of accountability.

f.3. **Training and Awareness:** Employees will receive training on the importance of NDAs and the role they play in protecting personal information. This training will emphasize the ethical and legal responsibilities of data handling.

g. Review of the Privacy Manual

WMSU's Privacy Manual will be reviewed and updated annually to ensure alignment with current data privacy best practices and legal requirements:

g.1. **Regular Evaluation:** The university will conduct regular evaluations of the Privacy Manual to assess its effectiveness and relevance in light of evolving privacy laws and emerging threats.

g.2. **Stakeholder Involvement:** Updates to the Privacy Manual will involve input from key stakeholders, including the DPO, COPs, and university leadership. This collaborative approach ensures that the manual reflects the needs and priorities of the entire university community.

g.3. **Continuous Improvement:** The review process will identify opportunities for continuous improvement and innovation in data privacy practices. This commitment to improvement ensures that WMSU remains at the forefront of data protection efforts.

Section 7.2: Physical Security Measures

a. Data Formats

WMSU recognizes the importance of securing personal information in both digital and physical formats:

a.1. **Digitization and Backup:** To ensure ease of access and data recovery, pertinent paper-based documents will be digitized and stored in secure data servers. This digitization process provides a backup mechanism and facilitates efficient data management.

a.2. **Secure Handling:** Both digital and paper-based documents will be handled with care to prevent unauthorized access or loss. The university will implement strict protocols for data handling, storage, and disposal to maintain data integrity and confidentiality.

b. Storage and Location

The physical storage of personal information at WMSU will adhere to strict security standards:

b.1. **Secure Storage Facilities:** Personal information in paper-based format will be stored securely in locked filing cabinets or dedicated data storage facilities. These facilities will be accessible only to authorized personnel to prevent unauthorized access or tampering.

b.2. **Access Control Measures:** WMSU will implement access control measures to restrict entry to storage facilities. These measures may include keycard access, biometric verification, and visitor logs to monitor and control access to sensitive areas.

c. Access Control

WMSU will establish a comprehensive access control framework to regulate access to data storage facilities:

c.1. **Access Control Policies:** Unit heads will develop and enforce access control policies that define access privileges and procedures. These policies will be based on a standard template approved by the DPO and tailored to the specific needs of each unit.
c.2. **Authorization Protocols:** Access to data storage facilities will be granted only to personnel with legitimate business needs. Authorization protocols will include verifying the identity and role of individuals seeking access and documenting access requests.
c.3. **Periodic Reviews:** Access control measures will be subject to periodic reviews to ensure their effectiveness and alignment with changing security requirements. These reviews will identify potential gaps and inform adjustments to access policies.

d. Access Documentation

WMSU will maintain comprehensive records of authorized access to personal information:

d.1. **Access Logs:** Access logs will document the names of personnel accessing personal information, along with the date, time, duration, and purpose of access. These logs will provide a detailed record of data access and facilitate monitoring and auditing efforts.
d.2. **Accountability and Transparency:** Access documentation will promote accountability and transparency in data handling practices. WMSU will use access logs to investigate unauthorized access attempts and take corrective action when necessary.
d.3. **Retention and Review:** Access logs will be retained for a specified period to support compliance and auditing requirements. Regular reviews of access logs will identify trends and inform security enhancements.

e. Office and Facility Layout

WMSU will optimize office and facility layouts to enhance data privacy and security:

e.1. **Secure Data Server Locations:** The DPO will coordinate with the MISTO to ensure that critical data server facilities are strategically located to minimize exposure to natural and human hazards. This includes evaluating site security, environmental conditions, and infrastructure resilience.
e.2. **Office Design Considerations:** Offices handling personal information will be designed to promote privacy and confidentiality. This includes positioning computers with adequate space between workstations, implementing privacy screens, and configuring office layouts to limit visual and auditory access to sensitive data.
e.3. **Safety and Security Measures:** The university will implement safety and security measures, such as fire suppression systems, climate control, and physical barriers, to protect data storage facilities and equipment.

Section 7.3: Technical Measures

a. Intrusion Detection Systems

WMSU will deploy robust technical measures to safeguard its digital infrastructure:

a.1. **Antivirus Software:** All university computers connected to the network will be equipped with up-to-date antivirus software to detect and mitigate malware threats. This proactive approach prevents unauthorized access and data corruption.
a.2. **Network Firewalls:** A comprehensive network firewall will be in place to protect WMSU's information systems and databases from external threats and unauthorized access attempts. The firewall will serve as a barrier against network-based attacks, enhancing the university's cybersecurity posture.
a.3. **Continuous Monitoring:** The Management Information Systems Technology Office (MISTO) will regularly monitor firewall logs to detect suspicious activities or security breaches. This continuous monitoring enables early detection and response to potential threats, minimizing the risk of data breaches.

b. Data Backup Procedures

WMSU will implement robust data backup procedures to ensure data availability and recoverability:

b.1. **Routine Backups:** The MISTO team will conduct routine data backups to create redundant copies of critical information. Full backups will be performed daily, while differential backups will be conducted as frequently as needed to capture incremental changes.
b.2. **Remote Backup Locations:** Backup data will be stored in remote locations separate from the primary data servers to enhance resilience against disasters and system failures. For

example, backup facilities may be situated in different university campuses to ensure geographical redundancy.

b.3. **Backup Management:** The MISTO team will manage backup operations to ensure backup facilities are secure and equipped to handle data recovery needs. Backup management will include regular testing of backup systems to verify data integrity and availability.

c. Security Controls Assessment

WMSU will conduct regular assessments of its technical security controls to ensure their effectiveness:

c.1. **Vulnerability Assessments:** The university will perform vulnerability assessments on critical systems, such as the network firewall and information systems, to identify potential weaknesses and vulnerabilities. These assessments will inform the development of mitigation strategies to enhance security.

c.2. **Penetration Testing:** WMSU will conduct penetration testing to simulate real-world attacks and evaluate the resilience of its security controls. Penetration testing provides valuable insights into potential attack vectors and informs the implementation of additional safeguards.

CHAPTER 8. BREACH AND SECURITY INCIDENTS

Section 8.1: Creation of a Data Breach Response Team

Western Mindanao State University (WMSU) shall establish a Data Breach Response Team (DBRT) tasked with the mitigation, management, and resolution of security incidents and personal data breaches. The DBRT will be under the direct supervision of the WMSU Data Protection Officer (DPO) and will include key personnel such as the Director for Management Information and Systems Technology Office (MISTO), Chief Administrative Officer and representatives from relevant departments.

The DBRT is responsible for:

a. Conducting initial assessments of incidents or breaches to ascertain their nature and extent.
b. Executing measures to mitigate the adverse effects of the incident or breach.
c. Restoring the integrity of the information and communication systems.
d. Ensuring compliance with the Data Privacy Act of 2012, its Implementing Rules and Regulations, and related issuances by the National Privacy Commission (NPC).

Section 8.2: Measures to Prevent and Minimize Occurrence of Breach and Security Incidents

To minimize the occurrence of breaches and security incidents, the following preventive measures shall be implemented:

a. Privacy Impact Assessments (PIA)

The DBRT shall regularly conduct PIAs to identify risks in the processing systems and monitor security breaches.

b. Vulnerability Scanning

Regular vulnerability scanning of WMSU's computer networks shall be conducted to detect potential security weaknesses.

c. Training and Capacity Building

Personnel involved in processing personal information must attend training sessions and seminars to enhance their skills and awareness of data protection.

d. Access Control

Access to data centers and sensitive information shall be regulated with appropriate security clearances and access control lists.

Section 8.3: Incident Response Procedure

In the event of a suspected or actual security incident or personal data breach, the following steps must be taken:

a. Immediate Reporting

Any suspected or actual security incident must be reported immediately to any member of the DBRT.

b. Initial Assessment

A team member shall conduct an initial assessment to verify the report and determine the incident's nature and extent.

c. Containment

The team shall contain the security incident to prevent further damage.

d. Restoration

Restore the integrity of affected information systems.

e. Mitigation

Implement measures to mitigate possible harm or negative consequences.

f. Notification

Notify relevant parties, including the NPC and affected data subjects, within 72 hours of knowledge of the breach.

Section 8.4: Notification Protocol

When a personal data breach requiring notification occurs, WMSU must notify the NPC and affected data subjects within seventy-two (72) hours. Notification is required when sensitive personal information or other information that may enable identity fraud is reasonably believed to have been acquired by an unauthorized person, and it is likely to pose a real risk of serious harm.

The notification shall include:

a. A description of the nature of the breach.
b. The personal data possibly involved.
c. Measures taken to address the breach and reduce harm.
d. Contact details of WMSU representatives from whom data subjects can obtain additional information.
e. Any assistance provided to affected data subjects.

Notification may be delayed only to determine the scope of the breach, prevent further disclosures, or restore system integrity.

Section 8.5: Documentation and Reporting Procedure

The DBRT shall prepare detailed documentation of every incident or breach encountered. Reports must include:

a. Description of the nature of the breach.
b. Personal information possibly involved.
c. Measures undertaken to address the breach.
d. Contact details of the personal information controller for additional information and assistance.

The documentation should be submitted to the Vice-President for Administration, the University President, and the NPC within the prescribed period. Annual reports summarizing security incidents and breaches shall also be prepared for internal review and submission to the NPC.

CHAPTER 9: INQUIRIES AND COMPLAINTS

Section 9.1: Inquiries

Western Mindanao State University (WMSU) is committed to transparency and ensuring that data subjects have access to information about their personal data. The following procedures are in place for inquiries:

a. Communication Channels

The Office of the Data Protection Officer (DPO) at WMSU provides both physical and digital channels for communication between the DPO and data subjects.

b. Submitting Inquiries:

b.1. **Email:** Data subjects may send an email to the DPO's office at dpo@wmsu.edu.ph to request information about the processing of their personal data under the university's custody.

b.2. **In-Person Visits:** Alternatively, data subjects may visit the DPO's office and submit a printed copy of their inquiry letter. The letter should include their contact details for reference.

c. Rights of Data Subjects:

c.1. Data subjects have the right to reasonable access to their personal data being processed by WMSU.

c.2. They may inquire about data privacy and security policies implemented to protect their personal data.|

Section 9.2: Complaints

WMSU provides a structured process for addressing complaints related to the processing of personal data:

a. Filing Complaints

a.1. All complaints related to data protection and privacy must be submitted first to the Data Protection Office, which serves as the University's designated office for handling such matters.

a.2. Complaints should be filed in three (3) printed copies and submitted directly to the Office of the DPO.

a.3. Complaints may also be filed electronically through dpo@wmsu.edu.ph**.**

b. Complaint Acknowledgment

The DPO will issue an acknowledgment receipt to the complainant upon receipt of the complaint.

c. Internal Investigation

c.1. Upon validation of the complaint, the DPO shall initiate an internal investigation, coordinate with the concerned offices, and recommend corrective measures to address the issue.

c.2. Resolution shall be made within fifteen (15) calendar days from receipt of the complaint. In exceptional cases requiring further investigation, the period may be extended up to thirty (30) calendar days, provided that the complainant is duly informed—whether in writing, through email, or by a formal phone call—of the reason for the extension

d. Exhaustion of Remedies and Escalation to the NPC

d.1. If the complaint is not resolved within a reasonable time or if the complainant is not satisfied with the resolution, the data subject may then escalate the complaint to the National Privacy Commission (NPC).

d.2. In the event of a confirmed personal data breach, the DPO shall report the incident to the NPC within seventy-two (72) hours from official knowledge of the breach, as required under the DPA and NPC regulations.

Section 9.3: Rights of Data Subjects

Data subjects at Western Mindanao State University (WMSU) are entitled to the full protection of their rights under the Data Privacy Act of 2012, its Implementing Rules and Regulations, and relevant issuances of the National Privacy Commission (NPC). These rights include the following:

a. Right to be Informed

Data subjects shall be informed whenever their personal data is being collected and processed by WMSU. They must be provided with clear information on what data is being collected, the purpose of processing, how it will be used, who will process or share it, and their rights as data subjects.

b. Right to Object

Data subjects may object to the processing of their personal data, particularly for purposes that are not related to academic, administrative, research, extension, or legal obligations of the University. WMSU shall respect such objection unless there are overriding legitimate grounds (e.g., compliance with laws, contracts, or vital interests).

c. Right to Access

Data subjects may request reasonable access to their personal data held by WMSU, including the sources of such data, the manner of processing, and any individuals or entities with whom the data is shared.

d. Right to Rectification (Correction of Errors)

Data subjects may dispute inaccuracies and request the correction of any incorrect, outdated, or misleading personal data kept by WMSU. WMSU shall take appropriate measures to ensure that inaccurate or incomplete data is promptly rectified.

e. Right to Erasure or Blocking (Right to be Forgotten)

Data subjects may request the suspension, withdrawal, blocking, or removal of their personal data when it is no longer necessary, consent has been withdrawn, or the data was unlawfully obtained.

However, under RA 9470 and NAP guidelines, government records (including those in SUCs) may only be disposed of in accordance with an approved Records Disposition Schedule (RDS/GRDS) and with prior written authority from the National Archives of the Philippines.

f. Right to Data Portability

Data subjects may obtain a copy of their personal data in a structured, commonly used, and machine-readable format. They may also request that WMSU transmit such data to another personal information controller, where technically feasible.

g. Right to Complain

Data subjects must first file their complaint with the Data Protection Office of WMSU for resolution. If not addressed within the prescribed period, they may then escalate the matter to the National Privacy Commission (NPC).

h. Right to Damages

Data subjects have the right to be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of their personal data. WMSU shall recognize and respect this right in accordance with applicable laws and regulations.

Section 9.4: Procedure for Inquiries and Complaints

WMSU ensures that all inquiries and complaints are handled promptly and effectively:

a. Inquiry Submission:

Data subjects may inquire or request information about any matter related to their personal data processing, including the data privacy and security policies in place at WMSU. All inquiries shall be addressed to the Data Protection Office, which serves as the University's focal office for data privacy compliance.

b. Complaint Handling:

Complaints should be submitted in writing, either in printed form or electronically. All complaints must be formally filed with the Data Protection Office, which will confirm receipt of the complaint and take the necessary action to address the issue in coordination with the concerned department or unit. The Office shall also maintain a record of all complaints and their resolutions to ensure accountability and continuous improvement in data privacy practices.

CHAPTER 10. MANUAL REVIEW AND UPDATE

a. This Data Privacy Manual shall be subject to regular review and revision to ensure its continued relevance, effectiveness, and alignment with applicable laws, regulations, and institutional policies.
b. The Data Protection Officer (DPO), in coordination with the Data Privacy Committee, shall initiate a comprehensive review of the Manual at least once every two (2) years or as may be necessary in response to significant changes in data privacy laws, relevant issuances from the National Privacy Commission (NPC), technological advancements, institutional processes, or after the occurrence of a data breach or privacy-related incident.
c. Proposed amendments shall be submitted to the appropriate authorities for evaluation and shall take effect only upon the approval of the Western Mindanao State University (WMSU) Board of Regents.
d. All personnel and relevant stakeholders shall be duly informed of any revisions to this Manual.

CHAPTER 11: EFFECTIVITY

This Data Privacy Manual was approved by the Western Mindanao State University (WMSU)Board of Regents under Board Resolution No. 101, Series of 2025, and shall take effect on October 10, 2025.

It shall remain in force until amended, revised, or repealed by the same authority.