

University of Science and Technology
of Southern Philippines
Alubijid | Cagayan de Oro | Claveria | Jasaan | Oroquieta | Panaon

THE USTP DATA PRIVACY MANUAL

TABLE OF CONTENTS

| | |
|----------|---|
| PART 1. | BACKGROUND |
| PART 2. | INTRODUCTION |
| PART 3. | DEFINITION OF TERMS |
| PART 4. | SCOPE AND LIMITATIONS |
| | <i>Section 1. Scope</i> |
| | <i>Section 2. Limitations</i> |
| PART 5. | DATA PRIVACY PRINCIPLES |
| | <i>Section 1. Principles of Transparency, Legitimate Purpose and Proportionality</i> |
| | <i>Section 2. General Principles for Collection, Processing, and Retention of Personal Data</i> |
| | <i>Section 3. General Principles for Data Sharing</i> |
| PART 6. | PROCESSING OF PERSONAL DATA |
| | <i>Section 1. Lawful Processing of Personal Information</i> |
| | <i>Section 2. Sensitive Personal and Privileged Information</i> |
| | <i>Section 3. Extension of Privileged Communication</i> |
| PART 7. | SECURITY MEASURES |
| | <i>Section 1. Data Privacy and Security</i> |
| | <i>Section 2. Organizational Security Measures</i> |
| | <i>Section 3. Physical Security Measures</i> |
| | <i>Section 4. Guidelines for Technical Security Measures</i> |
| PART 8. | SECURITY OF SENSITIVE PERSONAL INFORMATION |
| | <i>Section 1. Access to Sensitive Personal Information</i> |
| PART 9. | RIGHTS OF DATA SUBJECTS |
| | <i>Section 1. Rights of the Data Subject</i> |
| | <i>Section 2. Transmissibility of Rights of the Data Subject</i> |
| | <i>Section 3. Right to Data Portability</i> |
| | <i>Section 4. Limitation on Rights</i> |
| | <i>Section 5. Inquiries and Complaints</i> |
| PART 10. | DATA BREACH NOTIFICATION |
| | <i>Section 1. Data Breach Notification</i> |
| | <i>Section 2. Contents of Notification</i> |
| | <i>Section 3. Delay of Notification</i> |
| | <i>Section 4. Breach Report</i> |
| | <i>Section 5. Procedure for Notification</i> |

PART 11. OUTSOURCING AND SUBCONTRACTING AGREEMENTS

Section 1. Subcontract of Personal Data

Section 2. Agreements for Outsourcing

Section 3. Duty of Personal Information Processor

PART 12. RULES ON ACCOUNTABILITY

Section 1. Accountability for Transfer of Personal Data

Section 2. Accountability for Violations

PART 13. EFFECTIVITY

THE USTP DATA PRIVACY MANUAL

PART 1. BACKGROUND

Republic Act No. 10173 entitled “An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes”, or simply, Data Privacy Act of 2012 (DPA), is the law that gives form to the declared policy of the State to protect the fundamental human right of privacy and communication. It aims to protect personal data in information and communications systems both in the government and the private sector. While the State recognizes the vital role of information and communications technology in nation-building, it also acknowledges its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

Approved into law last August 15, 2012, the DPA created the National Privacy Commission (NPC) which is tasked to monitor its implementation. It covers the processing of personal information and sensitive personal information and sets, as its basic premise, the grant of direct consent by a data subject before data processing of personal information be allowed.

The law ensures that entities or organizations processing 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. The law serves the following purposes:

1. Protects the privacy of individuals while ensuring free flow of information to promote innovation and growth;
2. Regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data; and
3. Ensures that the Philippines complies with international standards set for data protection through the NPC.

Under the law, 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 or PIP is expected to produce a Privacy Manual (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 National Privacy Commission (NPC). It also encapsulates the privacy and data protection protocols that need to be

observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

PART 2. INTRODUCTION

In the free flow of information to promote innovation and growth, the fundamental human right of privacy and of communication must be protected. Information and communications technology has a vital role in nation-building. Personal information in information and communications systems in the University must be secured and protected.

The University of Science and Technology of Southern Philippines (USTP), in its commitment to uphold, respect and value data privacy rights, hereby adopts this Data Privacy Manual in compliance with the DPA, its Implementing Rules and Regulations (IRR), and other relevant policies, including issuances of the NPC. All personal data collected from all its officials, personnel, and clients shall be processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This Manual shall inform the clients/customers of the University's data protection and security measures, and may serve as the clients/customers' guide in exercising their rights under the DPA.

PART 3. DEFINITION OF TERMS

- a. *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 personal information about and/or relating to him/her. 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.
- b. *Data Sharing* – refers to 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.
- c. *Data Subject* – refers to an individual whose personal, sensitive personal or privileged information is processed by the University. It may refer to officers, employees, consultants, and clients/customers of the University.
- d. *Personal Data* – refers to all types of personal information.

- e. *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.
- f. *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 information, or when put together with other information would directly and certainly identify an individual.
- g. *Personal Information Controller (PIC)* – refers to an official/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 his/her 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.
- h. *Personal Information Processor (PIP)* – refers to any natural or juridical person qualified to act as such under the DPA and its IRR to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject.
- i. *Privileged Information* – refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.
- j. *Processing* – refers to any operation or any 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.
- k. *Sensitive Personal Information* – refers to personal information:
 - i. About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
 - ii. 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 person, the disposal of such proceedings, or the sentence of any court in such proceedings;
 - iii. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

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

PART 4. SCOPE AND LIMITATIONS

Section 1. Scope

This Manual applies to the processing of all types of personal information and to all officials, employees and personnel of the University, whether regular, contractual or project-based, who are involved in personal information processing in all the campuses, offices and units of the University.

This Manual is essentially an internal issuance and is meant for the use and application of the University's staff or personnel. All personnel of the University, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Manual.

Section 2. Limitations

This Manual does not apply to the following:

- a. 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:
 - i. The fact that the individual is or was an officer or employee of the government institution;
 - ii. The title, business address and office telephone number of the individual;
 - iii. The classification, salary range and responsibilities of the position held by the individual; and
 - iv. The name of the individual on a document prepared by the individual in the course of employment with the government;
- b. 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 his/her contract;
- c. 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: Provided, that they do not include benefits given in the course of an ordinary transaction or as a matter of right;

- d. Personal information processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations;
- e. Personal information that will be processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards;
- f. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law. Nothing in this Manual shall be construed as having amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);
- g. 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 (CISA), Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act, and other applicable laws; and
- h. 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 DPA and its IRR.

Provided, that the non-applicability of this Manual do not extend to PIC or PIP who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of this Manual only to the minimum extent necessary to achieve the specific purpose, function, or activity.

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.

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.

In all cases, the determination of any exemption shall be liberally interpreted in favor of the rights and interests of the data subject.

PART 5. DATA PRIVACY PRINCIPLES

The University, in the course of its operations, collects the basic contact information of its students, alumni, employees, personnel, suppliers, contractors, consultants and other clients, including their full name, address, email address, contact number, among others. The personal data collected shall be used by the University for purposes of documentation, recording and communication, among others. The University will 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.

All employees and personnel of the University 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 the University shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

Section 1. Principles of Transparency, Legitimate Purpose and Proportionality

The processing of personal information shall be allowed, subject to compliance with the requirements of this Manual and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality:

- a. *Transparency* – The data subject must be aware of the nature, purpose, and extent of the processing of his/her personal data, including the risks and safeguards involved, the identity of PIC, his/her rights as a data subject, and how these can be exercised. 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* – 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* – The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by any other means.

Section 2. General Principles for Collection, Processing, and Retention of Personal Data

The processing of personal data shall adhere to the following general principles in the collection, processing, and retention of personal data:

- a. Collection must be for a declared, specified, and legitimate purpose:

- i. Consent is required prior to the collection and processing of personal data, subject to exemptions provided by this Manual and other applicable laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn.
 - ii. The data subject must be provided specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his/her personal data for profiling or data sharing.
 - iii. Purpose should be determined and declared before, or as soon as reasonably practicable, after collection.
 - iv. Only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected.
- b. Personal data shall be processed fairly and lawfully:
 - i. 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.
 - ii. Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.
 - iii. Processing must be in a manner compatible with declared, specified, and legitimate purpose.
 - iv. Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
 - v. Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.
- c. Processing should ensure data quality:
 - i. Personal data should be accurate and where necessary for declared, specified and legitimate purpose, kept up to date.
 - ii. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.
- d. Personal data shall not be retained longer than necessary:
 - i. Retention of personal data shall only for as long as necessary:

- for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
 - for the establishment, exercise or defense of legal claims; or
 - for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.
- ii. Retention of personal data shall be allowed in cases provided by law.
- iii. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.
- e. Any authorized further processing shall have adequate safeguards:
- i. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organizational, physical, and technical security measures required by the DPA in order to safeguard the rights and freedoms of the data subject.
 - ii. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.
 - iii. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

Section 3. General Principles for Data Sharing

Further processing of personal data collected from a party other than the data subject shall be allowed under any of the following conditions:

- a. Data sharing shall be allowed when it is expressly authorized by law: *Provided*, that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose and proportionality.
- b. Data collected from parties other than the data subject for purpose of research shall be allowed when the personal data is publicly available, or has the consent of the data subject for purpose of research: *Provided*, that adequate safeguards are in place, and no decision directly affecting the data subject shall be made on the basis of the data collected or processed. The rights of the data subject shall be upheld without compromising research integrity.

- c. Data sharing between government agencies for the purpose of a public function or provision of a public service shall be covered by a *Data Sharing Agreement*.

PART 6. PROCESSING OF PERSONAL DATA

Section 1. Lawful Processing of Personal Information

Processing of personal information is allowed, unless prohibited by law. For processing to be lawful, any of the following conditions must be complied with:

- a. The data subject must have given his/her consent prior to the collection, or as soon as practicable and reasonable;
- b. The processing involves the personal information of a data subject who is a party to a contractual agreement, in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to entering the said agreement;
- c. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
- d. The processing is necessary to protect vitally important interests of the data subject, including his/life and health;
- e. The processing of personal information is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law;
- f. The processing of personal information is necessary for the fulfillment of the constitutional or statutory mandate of a public authority; or
- g. The processing is necessary to pursue the legitimate interests of the PIC, or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject, which require protection under the Constitution.

Section 2. Sensitive Personal and Privileged Information

The processing of sensitive personal and privileged information is prohibited, except in any of the following cases:

- a. Consent is given by data subject, or by the parties to the exchange of privileged information, prior to the processing of the sensitive personal information or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose;

- b. The processing of the sensitive personal information or privileged information is provided for by existing laws and regulations: Provided, that said laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data;
- c. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his/her consent prior to the processing;
- d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations provided that:
 - i. Processing is confined and related to the bona fide members of these organizations or their associations;
 - ii. The sensitive personal information are not transferred to third parties; and
 - iii. Consent of the data subject was obtained prior to processing;
- e. The processing is necessary for the purpose of medical treatment: Provided, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured; or
- f. The processing concerns sensitive personal information or privileged information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

Section 3. Extension of Privileged Communication

PICs may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered from privileged information is inadmissible.

PART 7. SECURITY MEASURES

Section 1. Data Privacy and Security

Security measures aim to maintain the availability, integrity and confidentiality of personal data and protect them against *natural dangers* such as accidental loss or destruction, and *human dangers* such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

PIC and PIP shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data. The PIC and PIP shall take steps to ensure that any natural person acting under their authority and who has access to personal data, does not process them except upon their instructions, or as required by law.

The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing. These measures shall be implemented 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.

Section 2. Organizational Security Measures

The University 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.

The University shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data. It may choose to outsource the conduct a PIA to a third party.

All employees will be asked to sign a Non-Disclosure Agreement. 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.

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

Where appropriate, PIC and PIP shall comply with the following guidelines for organizational security:

- a. *Compliance Officer* – The University shall designate an individual or individuals who shall function as Data Protection Officer (DPO). The DPO shall have the following functions and responsibilities:
 - i. Monitor the compliance by the PIC and the PIP with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies;
 - ii. Ensure the conduct of a Privacy Impact Assessment (PIA) relative to activities, measures, projects, programs, or systems of the PIC or PIP;
 - iii. Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights;

- iv. Ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
 - v. Inform and cultivate awareness on privacy and data protection within the University including all relevant laws, rules and regulations and issuances of the NPC;
 - vi. 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;
 - vii. Serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;
 - viii. Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security;
 - ix. Perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects;
 - x. Take charge in complying with the registration and compliance requirements of the NPC as prescribed under the DPA and its IRR, including the registration of personal data processing systems and notification of automated processing operations, as may be applicable, and submission of annual report of the summary of documented security incidents and personal data breaches; and
 - xi. Recommend for the approval of the PIC data privacy forms, including consent form, access request form, request for correction or erasure form, and privacy notices.
- b. *Conduct of Trainings/Seminars* – The University 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.
- c. *Conduct of Privacy Impact Assessment (PIA)* – The University shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data. It may choose to outsource the conduct a PIA to a third party.
- d. *Data Protection Policies* – Any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection

policies that provide for organization, physical, and technical security measures, and, for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects:

- i. The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.
 - ii. The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility.
 - iii. The policies shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices.
- e. *Records of Processing Activities* – Any natural or juridical person or other body involved in the processing of personal data shall maintain records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data. Records should include:
- i. Information about the purpose of the processing of personal data, including any intended future processing or data sharing;
 - ii. A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing;
 - iii. General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data;
 - iv. A general description of the organizational, physical, and technical security measures in place;
 - v. The name and contact details of the PIC and, where applicable, the joint controller, the its representative, and the compliance officer or DPO, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.
- f. *Management of Human Resources* – Any natural or juridical person or other entity involved in the processing of personal data shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data. The employees will be asked to sign a Non-Disclosure Agreement. All employees, agents, or representatives with access to

personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure. This obligation shall continue even after leaving the public service, transferring to another position, or upon terminating their employment or contractual relations. There shall be capacity building, orientation or training programs for such employees, agents or representatives, regarding privacy or security policies.

- g. *Processing of Personal Data* – Any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review:
 - i. A procedure for the collection of personal data, including procedures for obtaining consent, when applicable;
 - ii. Procedures that limit the processing of data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose;
 - iii. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems;
 - iv. Policies and procedures for data subjects to exercise their rights under the DPA; and
 - v. Data retention schedule, including timeline or conditions for erasure or disposal of records.
- h. *Contracts with Personal Information Processors (PIP)* – The PIC, through appropriate contractual agreements, shall ensure that its PIPs, where applicable, shall also implement the security measures required by this Manual. It shall only engage those PIPs that provide sufficient guarantees to implement appropriate security measures specified in this Manual, and ensure the protection of the rights of the data subject.
- i. *Review of Privacy Manual* – This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the University shall be updated to remain consistent with current data privacy best practices.

Section 3. Physical Security Measures

Physical security measures are intended to monitor and limit access to the facility containing the personal data, including the activities therein. They 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.

To ensure that mechanical destruction, tampering and alteration of personal data under the custody of the University are prevented, and that these data are protected from

man-made disasters, power disturbances, external access, and other similar threats, the following shall be observed:

- a. Personal data in the custody of the University shall be in digital/electronic format and paper-based/physical format.
- b. All personal data being processed by the University shall be stored in a data room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computers.
- c. Only authorized personnel shall be allowed inside the data room. For this purpose, they shall each be given a duplicate of the key to the room. Other personnel may be granted access to the room upon filing of an access request form with the DPO and the latter's approval thereof.
- d. All personnel authorized to enter and access the data room or facility must fill out and register with the online registration platform of the University, and a logbook placed at the entrance of the room. They shall indicate the date, time, duration and purpose of each access.
- e. The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.
- f. Persons involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their own gadgets or storage device of any form when entering the data storage room.
- g. 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.
- h. The University shall retain the personal data of a client/customer for a specific number of years from acquisition. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.

Where appropriate, PICs and PIPs shall comply with the following guidelines for physical security:

- a. Policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media;
- b. Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public;

- c. The duties, responsibilities and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time;
- d. Any natural or juridical person or other body involved in the processing of personal data shall implement policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of personal data;
- e. Policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

Section 4. Guidelines for Technical Security Measures

Each PIC and PIP must 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, as follows:

- a. The University shall use an intrusion detection system to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system.
- b. The University 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.
- c. The University shall review security policies, conduct vulnerability assessments and perform penetration testing within the company on regular schedule to be prescribed by the appropriate department or unit.
- d. Each personnel with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication.
- e. A Data Breach Response Officer (DBRO) shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The DBRO shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. He/she shall also execute measures to mitigate the adverse effects of the incident or breach.
- f. The University shall regularly conduct a PIA to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. 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 University.

- g. The University 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.
- h. The DBRO shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the DBRO.
- i. The DBRO shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period.

Where appropriate, PICs and PIPs shall adopt and establish the following technical security measures:

- a. A security policy with respect to the processing of personal data;
- b. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;
- c. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;
- d. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach;
- e. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- f. A process for regularly testing, assessing, and evaluating the effectiveness of security measures;
- g. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

PART 8. SECURITY OF SENSITIVE PERSONAL INFORMATION

All sensitive personal information maintained by the University shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the ICT industry.

Section 1. Access to Sensitive Personal Information

On-Site and Online Access:

- a. No employee of the government shall have access to sensitive personal information on government property or through online facilities unless he/she has received a security clearance from the University as the agency who originally collected the personal data.
- b. The University shall strictly regulate access to sensitive personal information under its custody or control, particularly when it allows online access. An employee of the government shall only be granted a security clearance when the performance of his/her official functions or the provision of a public service directly depends on and cannot otherwise be performed unless access to the personal data is allowed.
- c. Where allowed under the next preceding paragraphs, online access to sensitive personal information shall be subject to the following conditions:
 - i. An IT governance framework has been designed and implemented;
 - ii. Sufficient organizational, physical and technical security measures have been established;
 - iii. The agency is capable of protecting sensitive personal information in accordance with data privacy practices and standards recognized by the information and communication technology industry;
 - iv. The employee of the government is only given online access to sensitive personal information necessary for the performance of official functions or the provision of a public service.

Off-Site Access:

- a. Sensitive personal information maintained by an agency may not be transported or accessed from a location off or outside of government property, whether by its agent or employee, unless the head of agency has ensured the implementation of privacy policies and appropriate security measures. A request for such transportation or access shall be submitted to and approved by the head of agency. The request must include proper accountability mechanisms in the processing of data.

- b. The head of agency shall approve requests for off-site access in accordance with the following guidelines:
 - i. *Deadline for Approval/Disapproval.* The head of agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. Where no action is taken by the head of agency, the request is considered disapproved;
 - ii. *Limitation to 1,000 Records.* Where a request is approved, the head of agency shall limit the access to not more than one thousand (1,000) records at a time, subject to the next succeeding paragraph.
 - iii. *Encryption.* Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard recognized by the NPC.

PART 9. RIGHTS OF DATA SUBJECTS

Section 1. Rights of the Data Subject

The data subject is entitled to the following rights:

- a. *Right to be Informed*
 - i. The data subject has a right to be informed whether personal data pertaining to him/her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.
 - ii. The data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity:
 - Description of the personal data to be entered into the system;
 - Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
 - Basis of processing, when processing is not based on the consent of the data subject;
 - Scope and method of the personal data processing;
 - The recipients or classes of recipients to whom the personal data are or may be disclosed;

- Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
 - The identity and contact details of the personal data controller or its representative;
 - The period for which the information will be stored; and
 - The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the NPC.
- b. *Right to Object.* The data subject shall have the right to object to the processing of his/her personal data, including processing for direct marketing, automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph.

When a data subject objects or withholds consent, the personal information controller shall no longer process the personal data, unless:

- i. The personal data is needed pursuant to a subpoena;
 - ii. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
 - iii. The information is being collected and processed as a result of a legal obligation.
- c. *Right to Access.* The data subject has the right to reasonable access to, upon demand, the following:
- i. Contents of his/her personal data that were processed;
 - ii. Sources from which personal data were obtained;
 - iii. Names and addresses of recipients of the personal data;
 - iv. Manner by which such data were processed;
 - v. Reasons for the disclosure of the personal data to recipients, if any;

- vi. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
 - vii. Date when his or her personal data concerning the data subject were last accessed and modified; and
 - viii. The designation, name or identity, and address of the personal information controller.
- d. *Right to Rectification.* The data subject has the right to dispute the inaccuracy or error in the personal data and have the PIC correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the PIC shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: Provided, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.
- e. *Right to Erasure or Blocking.* The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his/her personal data from the PIC's filing system.
- i. This right may be exercised upon discovery and substantial proof of any of the following:
 - The personal data is incomplete, outdated, false, or unlawfully obtained;
 - The personal data is being used for purpose not authorized by the data subject;
 - The personal data is no longer necessary for the purposes for which they were collected;
 - The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
 - The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
 - The processing is unlawful;
 - The PIC or PIP violated the rights of the data subject.

- ii. The PIC may notify third parties who have previously received such processed personal information.
- f. *Right to Damages.* The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his/rights and freedoms as data subject.

Section 2. Transmissibility of Rights of the Data Subject

The lawful heirs and assigns of the data subject may invoke the rights of the data subject to which he/she is an heir or an assignee, at any time after the death of the data subject, or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

Section 3. Right to Data Portability

Where his/her personal data is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the PIC a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject. The exercise of this right shall primarily take into account the right of data subject to have control over his/her personal data being processed based on consent or contract, for commercial purpose, or through automated means. The NPC may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

Section 4. Limitation on Rights

The immediately preceding sections shall not be applicable if the processed personal data are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: Provided, that the personal data shall be held under strict confidentiality and shall be used only for the declared purpose. The said sections are also not applicable to the processing of personal data gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject. Any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research or investigation.

Section 5. Inquiries and Complaints

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

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the University, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the University using official email, and briefly discuss the inquiry, together with their contact details for reference.

Complaints shall be filed in three (3) printed copies, or sent to official email. The concerned office shall confirm with the complainant its receipt of the complaint.

PART 10. DATA BREACH NOTIFICATION

Section 1. Data Breach Notification

The NPC and affected data subjects shall be notified by the PIC within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred.

Notification of personal data breach shall be required when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the PIC or the NPC believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

Depending on the nature of the incident, or if there is delay or failure to notify, the NPC may investigate the circumstances surrounding the personal data breach. Investigations may include on-site examination of systems and procedures.

Section 2. Contents of Notification

The notification shall at least describe the nature of the breach, the personal data possibly involved, and the measures taken by the entity to address the breach. The notification shall also include measures taken to reduce the harm or negative consequences of the breach, the representatives of the PIC, including their contact details, from whom the data subject can obtain additional information about the breach, and any assistance to be provided to the affected data subjects.

Section 3. Delay of Notification

Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

In evaluating if notification is unwarranted, the NPC may take into account compliance by the PIC with this section and existence of good faith in the acquisition of personal data.

The NPC may exempt a PIC from notification where, in its reasonable judgment, such notification would not be in the public interest, or in the interest of the affected data subjects.

The NPC may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Section 4. Breach Report

The PIC shall notify the NPC by submitting a report, whether written or electronic, containing the required contents of notification. The report shall also include the name of a designated representative of the PIC, and his/her contact details.

All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of personal data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the PIC. In other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the NPC. A general summary of the reports shall be submitted to the NPC annually.

Section 5. Procedure for Notification

The Procedure for breach notification shall be in accordance with the DPA and its IRR, and any other issuance of the NPC.

PART 11. OUTSOURCING AND SUBCONTRACTING AGREEMENTS

Section 1. Subcontract of Personal Data

A PIC may subcontract or outsource the processing of personal data: Provided, that the PIC shall use contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the DPA and its IRR, other applicable laws for processing of personal data, and other issuances of the NPC.

Section 2. Agreements for Outsourcing

Processing by a PIP shall be governed by a contract or other legal act that binds the PIP to the PIC.

The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the PIC, and the geographic location of the processing under the subcontracting agreement.

The contract or other legal act shall stipulate, in particular, that the PIP shall:

- a. Process the personal data only upon the documented instructions of the PIC, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;
- b. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data;
- c. Implement appropriate security measures and comply with the DPA and its IRR, and other issuances of the NPC;
- d. Not engage another processor without prior instruction from the PIC: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;
- e. Assist the PIC, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;
- f. Assist the PIC in ensuring compliance with the DPA and its IRR, other relevant laws, and other issuances of the NPC, taking into account the nature of processing and the information available to the PIP;
- g. At the choice of the PIC, delete or return all personal data to the PIC after the end of the provision of services relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the DPA or another law;
- h. Make available to the PIC all information necessary to demonstrate compliance with the obligations laid down in the DPA, and allow for and contribute to audits, including inspections, conducted by the PIC or another auditor mandated by the latter; and
- i. Immediately inform the PIC if, in its opinion, an instruction infringes the DPA and its IRR, or any other issuance of the NPC.

Section 3. Duty of Personal Information Processor

The PIP shall comply with the requirements of the DPA and its IRR, other applicable laws, and other issuances of the NPC, in addition to obligations provided in a contract, or other legal act with a PIC.

PART 12. RULES ON ACCOUNTABILITY

Section 1. Accountability for Transfer of Personal Data

A PIC shall be responsible for any personal data under its control or custody, including information that have been outsourced or transferred to a PIP or a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

A PIC shall be accountable for complying with the requirements of the DPA and its IRR, and other issuances of the NPC. It shall use contractual or other reasonable means to provide a comparable level of protection to the personal data while it is being processed by a PIP or third party.

A PIC shall designate an individual or individuals who are accountable for its compliance with the DPA. The identity of the individual or individuals so designated shall be made known to a data subject upon request.

Section 2. Accountability for Violations

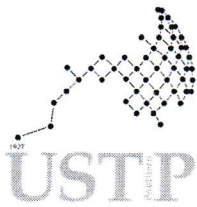
Any natural or juridical person, or other body involved in the processing of personal data, who fails to comply with the DPA and its IRR, and other issuances of the NPC, shall be liable for such violation, and shall be subject to its corresponding sanction, penalty, or fine, without prejudice to any civil or criminal liability, as may be applicable.

In cases where a data subject files a complaint for violation of his/her rights as data subject, and for any injury suffered as a result of the processing of his/her personal data, the NPC may award indemnity on the basis of the applicable provisions of the New Civil Code.

In case of criminal acts and their corresponding personal penalties, the person who committed the unlawful act or omission shall be recommended for prosecution by the NPC based on substantial evidence.

PART 13. Effectivity

The provisions of this Manual are effective upon approval by the Board of Regents.



University of Science and Technology of Southern Philippines

Alubijid | Cagayan de Oro | Claveria | Jasaan | Oroquieta | Panaon

Office of the BOR Secretary


University System

SECRETARY'S CERTIFICATE

THIS IS TO CERTIFY that based on the records of this office, during the meeting of the Board of Regents of the University of Science and Technology of Southern Philippines held on March 18, 2019 at the CHED Central Office, HEDC Bldg., CP Garcia Avenue, Diliman, Quezon City, whereat a quorum was present, **Resolution No. 19, S. 2019** was passed with the following dispositive portion:

“WHEREFORE THE BOARD OF REGENTS RESOLVED TO APPROVE THE DATA PRIVACY MANUAL OF THE UNIVERSITY AS ENDORSED BY THE ADMINISTRATIVE COUNCIL THROUGH ADCO RESOLUTION NO. 12, S. 2019 DATED MARCH 12, 2019.”

Issued this 25th day of March, 2019 at the Office of the University and Board Secretary, USTSP Cagayan de Oro Campus, Cagayan de Oro City.


CLINT DJANGO G. PACANA
University and Board Secretary