University of Southeastern Philippines
Knowledge Management Systems Division

Data Privacy Manual

PART 3. DEFINITION OF TERMS

a. ***Data Subject***

i.

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

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 information, including the risks and safeguards involved, the identity of PIC, his/her rights as a data subject, and how these can be exercised. Any

l. Alumni's personal information

Other personal information not listed above may be collected when there is a legitimate purpose for the collection of such.

3. Contexts and modes of data collection

a. University entrance application

The University Guidance and Testing Office (UGTO) collects the necessary personal and academic information of applicants as prerequisite for the University's admission test (USePAT). These information shall be used to verify the identity of applicants and evaluate their eligibility to take the USePAT. Data collection in this context may involve data entry in official paper-based, digital, and/or online web forms.

b. Student admission or enrolment

The Office of the University Registrar (OUR) collects the necessary personal information and pertinent documents bearing such as prerequisite for official admission to the University. This data collection is in compliance with the CHED Memorandum Order No. 30, series of 2009 and in accordance with the Manual of Regulations for Private Higher Education (MORPHE) of 2008.

c. Student academic evaluation

Throughout the entire academic life of students in the University, their academic ratings or grades shall be evaluated and collected as the primary means for evaluating their progress and qualification for graduation.

d. Employee application and management

The Human Resource Management Division (HRMD) collects the personal information of individuals who apply for employment in the University. These information are used to verify the identity of the applicants and evaluate their qualification for the position they are applying for.

The HRMD also handles and manages the personal information of all University employees as part of its institutional and legal obligations.

e. Visitor identification

Individuals who are not in any way affiliated with the University but may present a valid reason for entrance to its campuses, offices, and/or facilities are required to present their personal information and some valid proof of identification to the University's Security Service Unit (SSU) for security purposes.

ii. Information systems

The PQUaRM Division, in coordination with the Knowledge Management System Division (KMSD) and the Office of the DPO, shall specify the information system(s) relevant to a particular procedure and such shall be made accessible to the designated process owner. Process owners shall only process personal information through the information systems they are officially given access to.

iii. Scope and interoperability of information systems

The scope of an information system must be clearly and comprehensively defined especially since the University mostly uses a centralized database system to handle the data of its information systems. A document specifying the Personal information elements of

d. Lawful destruction of personal information

Retained personal information shall be securely and properly disposed of after it has served its purpose. No personal information shall be destroyed unless authorized by law and the University.

e. Data disposal protocol

The University shall adhere to the provisions in the National Archives of the Philippines Act of 2007 (R.A. 9470) in the disposal of official public records containing personal information.

i. Approval and documentation

Disposal of personal and/or sensitive data stored in physical and/or digital form contained in an official public document shall

iv. Shredding of paper-based documents

Offices which often deal with personal information stored in paper-based documents shall have at least one paper shredder at their disposal. Paper documents that contain personal information must be shredded once there is no longer a legitimate purpose for keeping them. Documents of this nature shall never be recycled or used for purposes other than what they were initially intended for. For documents classified as official public record, the disposal protocol shall be done in accordance with the National Archives of the Philippines Act of 2007 (R.A 9470).

PART 7. DISCLOSURE OF PERSONAL INFORMATION

All University personnel and employees shall practice due diligence and utmost care in handling personal information. The University shall never share or disclose data to third parties without prior consent from the data subjects. Whenever disclosure of data is necessary and permitted, the University shall conscientiously review the privacy and security policies of the authorized third-party service providers or external partners. The University may also be required to disclose data in compliance with legal or regulatory obligations.

a. Perpetuity of confidentiality

Even after an employee's termination of contract with the University, he/she shall maintain the confidentiality and secrecy of all personal information that he/she has knowledge of. The same applies to students, alumni or any other individual who had been officially allowed by the University to collect and/or process personal information for legitimate purposes (e.g. student council, campus organizations, etc.).

b. Internal data sharing

Internal disclosure of personal information from one unit to another within the University shall be subjected to an institutionalized standard data request procedure. This ensures that data is transmitted through official channels and shared for legitimate purposes. The data request form to be used in such procedure shall include details regarding the requesting entity, requested data, justification for such request, date, and signature of the requesting individual.

c. External data sharing

Data sharing to external entities shall only be allowed when it is expressly authorized by law and/or the data subject has consented to such activity. In such cases, a *Data Sharing Agreement* must be crafted to clearly specify the extent and nature of personal information disclosure and ensure that adequate safeguards are in place. For every University endeavor that requires a Memorandum of Agreement

(MOA) or Memorandum of Understanding (MOU) and involves the disclosure or processing of personal information, a data sharing agreement must be agreed upon by the University and the external party.

d. Public disclosure of personal information

Disclosing the personal information of students and employees without legitimate purpose and legal basis shall not be allowed. Upon official entry to the University, students and employees shall be informed of the extent at which the University may disclose their personal information inherent in the University's function and interests as an academic institution and a government organization. For instance, the University may publicly disclose, in all of its official channels, the personal information of a student who has won a competition representing the University.

However, the University shall have no automatic right to publicly disclose the personal information of a student relative to his/her accomplishment(s) if he/she did not officially represent the University in the particular event or he/she is not officially affiliated with the University at the time the event was held.

Example: Posting of personal information in social media

University employees must refrain from publicly posting personal

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-a-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; and

ix.

c) Conducting Relevant Trainings or Seminars

PART 12. SEPARABILITY CLAUSE

If for any reason, any portion or provision of this Manual be declared unconstitutional, other parts or provisions thereof which are not affected thereby shall continue to be in full force and effect.

PART 13. EFFECTIVITY

The provisions of this Manual are effective upon the approval of the University's Board of Regents.

PART 14. ANNEXES

Annex A

University of Southeastern Philippinesôs Data Privacy Statement

The right to privacy is a fundamental human right. Acknowledging this, the University of Southeastern Philippines, hereafter referred to as "University", endeavors to safeguard its stakeholders' data privacy by adhering to data privacy principles and employing standard safety measures in the collection, processing, disclosure and retention of Personal information in accordance with the Data Privacy Act of 2012 (R.A. 10173), its Implementing Rules and Regulations (IRR) and to issuances of the National Privacy Commission.

This University Data Privacy Statement (the "UDPS") contains an outline of the general practices of the University in the context of data collection and processing. All other data privacy statements released or to be released by the University specific to a particular office, function or procedure shall be in congruence with the UDPS. Designed for general knowledge, the UDPS may not include specific information pertaining to the data collection and processing mechanism of a specific office, function or procedure. Thus, whenever applicable, a more specific data privacy statement or notice should be consulted.

For a comprehensive and detailed view of the University's data privacy policies, please refer to the University's Data Privacy Manual.

What Personal information the University may collect and process?

The University collects and processes only the type and amount of data necessary to perform its core and auxiliary functions. As an institution composed of heterogeneous entities, the University may collect a variety of personal information in different contexts and for different specific purposes.

In general, among the common Personal information the University may collect include:

Name
Specimen signatures
Home address
Email address
Biographical information
Academic information
Nationality
Phone number

Images via CCTV and other similar recording devices
Internet Protocol (IP) addresses
Cookie session data

As a premiere research institution, the University may also collect sensitive personal information in the conduct of relevant researches and studies. For instance, a University-affiliated researcher may collect data pertaining to an individual's ethnic origin, political opinions or criminal history to achieve the objectives of a particular study.

All Personal information collection and processing can only be done when the University acquires the consent of the data subject, either explicitly or implicitly, after the latter has been informed of the nature and extent of data collection and processing.

Why does the University collect and process Personal information?

The purpose of Personal information collection and processing may vary from one University procedure (e.g. student admission, visitor entry, human resource management, etc.) to another.

Internal disclosure of Personal information from one unit to another within the University shall be subjected to an institutionalized standard data request procedure. This ensures that data is transmitted through official channels and shared for legitimate purposes.

Regardless of the context of data disclosure, the University shall always practice the principle of data minimization which means that only the minimum amount of data needed to serve a particular purpose is shared to the requesting entity.

How does the University protect Personal information?

The University shall employ necessary or reasonable safeguards in the form of physical, technological, logical and administrative controls. Internal access to stored Personal information will be kept to a minimum number of authorized individuals and bounded by confidentiality agreements. These individuals are subjected to regular training for proper handling of information in accordance to the University's data privacy policies and other related laws, regulations or issuances.

Annex B

CONSENT FORM

I have read the University of Southeastern Philippines' Data Privacy Statement

	malicious software. Unintentional collection of data by unauthorized personnel due to system glitch, lack of personnel training, and/or personnel incompetence. Intentional data collection by unauthorized personnel with or without malicious intent. Unintentional and unauthorized data collection by a legitimate University application due to system integration and scope issues.				

C06	Force majeure and other emergency events beyond the control of the University disable the collection of data through automated and/or manual means.	Low (1)	Medium (2)	2	**Preventive:** Define institutionalized contingency plans and emergency protocols in coordination with the university's general services unit. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.

.43Tm8og B/Fcuoaoaoa oa0)(-F5)(ge3Tm 0F10T10Tm 0)(-F92)(u c

					document the incident for purposes of investigation and prevention of future incidents of the same nature.
U02	Unauthorized processing of data subject data by an unauthorized system and/or personnel internal or external to the institution.	Medium (2)	High (3)	6	**Preventive:** Define a comprehensive and well-documented acceptable data use policy that should include provisions regarding process ownership, access rights and user privileges for each legitimate

					Mitigating: Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.
U04	Improper or incompetent use of the data processing system by qualified personnel that compromised the availability, integrity, and confidentiality of Personal information.	Low (1)	Medium (2)	2	**Preventive:** Institutionalize the regular conduct of personnel trainings, creation of user manuals, and the establishment of a technical support facility. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.

R02	Retained data are inaccurate and outdated.	Medium (2)	Medium (2)	4	**Preventive:** Define a comprehensive and well-documented data retention policy that should include, but may not be limited to, the following provisions: Coordination of development, quality assurance, and data privacy review teams to ensure that controls and measures are in place to guarantee the accuracy and currency of retained data especially in systems involving a centralized database. Regular monitoring and overseeing of retained data through a set of detective controls which may include or be a combination of: process, human capital, physical, and/or technological controls. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature. Specifically, This may entail the implementation of a data rectification and deletion procedure that should involve the process owners, development team, data privacy team, and top management.
R03	Retained data are modified by different users who have access privileges.	Low (1)	Medium (2)		

appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same

					Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.
DE02	Unauthorized disclosure of data by an unauthorized system and/or personnel internal or external to the institution.	Medium (2)	High (3)	6	**Preventive:** Define a comprehensive and well-documented data disclosure policy and protocol that should

					mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.

Definition

CRITERIA	LIKELIHOOD	SEVERITY	RATING
Low	Almost sure not to occur Not likely to occur	Negligible Minor impact/almost negligible	0 1
Medium	An even chance to occur	Moderate	2
High	Very likely to occur Extremely sure to occur	Critical Involving or sudden great damage or suffering	3 4

An action plan is required for risk factor ≥5