SAINT LOUIS UNIVERSITY

A. Bonifacio Street
Baguio City

DATA PRIVACY MANUAL

2019 Edition

I. INTRODUCTION AND GUIDING PHILOSOPHY

Saint Louis University (SLU) is committed to respect and protect the rights to data privacy of individuals. Towards this end, SLU is adopting this Data Privacy Manual to ensure that these rights are upheld, while at the same time being cognizant of the important role of data and information in achieving SLU's objective of delivering quality Catholic missionary education. Consequently, SLU shall balance the use of data and information to achieve its fundamental goal and ensure its legitimate interests as an educational institution, while at the same time protecting the data privacy rights of its stakeholders.

As an educational institution, SLU collects, processes, and stores information about its employees, applicants, students, parents and guardians, alumni, service providers, and other individuals for a variety of purposes. It is the policy of SLU that whatever information it gathers will be collected, processed and stored pursuant to the general principles of transparency, legitimate purpose, and proportionality, as mandated by Republic Act No. 10173 or the Data Privacy Act (DPA) of 2012, its Implementing Rules and Regulations, and other relevant data privacy issuances by the National Privacy Commission.

SLU's personal data processing activities shall always conform with the provisions of the DPA and all applicable Education Laws and Regulations, including, but not limited to, the Education Act of 1982 (Batas Pambansa Blg. 232), the Manual of Regulations for Private Higher Education (MORPHE), the Revised Manual of Regulations for Private Schools in Basic Education, relevant CHED Memorandum Orders, issuances by the Department of Education, issuances by the Legal Education Board, and other applicable laws, regulations, and administrative issuances in relation to education and privacy.

II. DEFINITION OF TERMS

Whenever used in this Manual, the following terms shall have the respective meanings hereinafter set forth:

- "*Data Privacy Act*" or "*DPA*" refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012, and its Implementing Rules and Regulations;
- "*NPC*" refers to the National Privacy Commission;
- "*SLU*" or "*University*" refers to Saint Louis University, Inc.;
- "*Organizational unit*" or "*unit*" or "*office*" refers to the various offices in the University, regardless of size or function. It includes the various Schools, Offices, Centers, Clinics, Institutes, Residence Halls, and other components of the University. It does not, however, include the foundations or institutes that are affiliated to, or were set up by, the University, which have their own separate juridical personality;
- "*Data subject*" refers to an individual whose personal, sensitive personal, or privileged information is processed by the University. For purposes of this Manual, the data subjects include, but are not limited to, employees, applicants, students, parents and guardians, alumni, service providers, and other individuals whose personal information is collected, processed, and stored by the University;
- "*Personal data*" refers to all types of personal information;
- *"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;

- *"Sensitive personal information"* refers to personal information:
    - 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 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;
    - 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,
    - specifically established by an executive order or an act of Congress to be kept classified;
- "*Privileged information*" refers to any and all forms of data, which, under the Rules of Court and other pertinent laws, constitute privileged communication;
- "*Personal information controller*" refers to one who controls the processing of personal data, or instructs another to process personal data on its behalf. In the context of this Manual, the personal information controller is SLU, comprising of the various organizational units that are involved in the processing of personal data of SLU's data subjects, such as:
    - the Human Resource Department;
    - the Finance Office;
    - the Technology Management and Development Department and its component units;
    - the Registrar's Office;
    - the Office of Student Affairs;
    - the Guidance Center;
    - the various Schools, including the Elementary and High Schools;
    - the Campus Planning, Maintenance, and Security Department;
    - the Legal Affairs Department;
    - the Campus Ministry and Parish Offices;
    - the University Clinics (Medical and Dental);
    - the Residence Halls; and,
    - all other units that are involved in the processing of personal data;
- "*Personal information processor*" refers to any natural or juridical person to whom the University may outsource or instruct the processing of personal data pertaining to SLU's data subjects. For purposes of this Manual, the personal information processors are the service providers whose services were contracted or outsourced by SLU to process personal data for the University. These include the providers of the systems for security, maintenance, Enterprise Resource Planning, ID/gate pass/car park, and such other contractors whose services are now or may hereafter be contracted by SLU for purposes of data processing;
- "*Processing*" refers to any operation or set of operations performed on personal data through automated or manual means, including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, and erasure or destruction of data;
- "*Consent of the data subject*" refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic, or recorded means. It

may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so.

- *"Personal data breach*" refers to a breach of security, whether accidental or intentional, that may lead to one or more of the following:
    - *confidentiality breach*, which results from the unauthorized or unlawful disclosure of, or access to, personal data;
    - *integrity breach*, which results from unauthorized or unlawful alteration or modification of personal data; and/or,
    - *availability breach*, which results from unauthorized or unlawful loss or destruction of personal data, or the denial of authorized or legitimate access to the same.
- "*Security incident*" is an event or occurrence that affects or tends to affect data protection, or may compromise the confidentiality, integrity, and availability of personal data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.

III. ORGANIZATIONAL STRUCTURE FOR DATA PROTECTION GOVERNANCE

A. *Data Protection Officer, Assistant Data Protection Officer*

Pursuant to the provisions of the DPA and NPC Advisory No. 2017-01, the University shall appoint a Data Protection Officer (DPO). At present, the Vice President for Administration acts as the DPO. In the event that another DPO is appointed by the University, the DPO shall be directly under the Office of the Vice President for Administration. The DPO shall be assisted by an Assistant Data Protection Officer (ADPO).

The DPO and ADPO shall be responsible for ensuring the University's compliance with applicable laws and regulations for the protection of data privacy and security. They shall oversee the performance of functions by the various organizational units in terms of their compliance with this Manual.

The functions and responsibilities of the DPO shall particularly include, among others, the following:

1. monitoring SLU's and its various units' compliance with the DPA, issuances by the NPC, and other applicable laws and policies;
2. ensuring the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or data processing systems of SLU and its various units;
3. advising SLU and its various units regarding complaints and/or the exercise by data subjects of their rights;
4. ensuring proper data breach and security incident management by SLU and its various units, including the preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
5. informing and cultivating awareness on privacy and data protection within SLU and its various units, including all relevant laws, rules and regulations and issuances of the NPC;
6. advocating for the development, review and/or revision of policies, guidelines, projects and/or programs of SLU and its various units relating to privacy and data protection, by adopting a privacy by design approach;
7. serving as the contact person of SLU vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns;

8. cooperating, coordinating and seeking the advice of the NPC regarding matters concerning data privacy and security; and,
9. performing other duties and tasks that will further the interest of data privacy and security and uphold the rights of the data subjects.

Except when the DPO expressly reserves unto himself the performance of some of the above-enumerated functions, the ADPO may perform all other functions of the DPO. The ADPO shall also be responsible for the operational and technical functions of the Data Protection Committee.

B. *The Data Protection Committee*

The Data Protection Committee (DPC) shall be SLU's policy-formulating body as well as the oversight committee on all matters related to data protection and privacy. All policies formulated by the DPC shall be reviewed by the Vice President for Administration, and subject to the final approval of the University President.

For proper coordination and functioning, the DPO, who shall serve as the Chair of the DPC, shall take charge of all policy-related directions of the University concerning data privacy. All policy-related issuances on data privacy shall be subject to the recommendation of the DPC, the favorable review by the Vice President for Administration, and the final approval of the University President.

The DPC shall be composed of the following regular members:

- the DPO as the Chair;
- the ADPO as member and technical consultant; and,
- the Campus Planning, Maintenance, and Security Department Director as member.

The heads of relevant organizational units shall serve as members of the DPC on an *ad-hoc* basis. They may be frequently consulted by the DPC regular members when crafting policies related to data privacy. They may likewise propose the adoption of certain policies for the consideration and deliberation of the DPC.

For operational purposes, the heads of the following units shall serve as the Secretariat of the DPC, and may be tapped by the DPC depending on the activity that would require the services and assistance of a secretariat:

- Human Resources Department
- Technology Management and Development Department
- Registrar's Office
- Office of Student Affairs

C. *The Data Protection Response Team*

The DPC, together with the heads of the appropriate units involved in the processing of personal data of SLU's data subjects, shall serve as the Data Protection Response Team (DPRT). It shall be the DPRT's responsibility to respond to inquiries and complaints relating to data privacy and security, and to assist in the monitoring and implementation of this Manual and the privacy policies of the various units.

D. *The Data Breach Response Team*

The DPC, together with the heads of the Human Resources Department, the Office of Student Affairs,

the Technology Management and Development Department, and the Legal Affairs Department shall serve as the Data Breach Response Team (DBRT). The DBRT shall formulate, implement, review, and revise as may be needed the security incident and personal data breach management policies of the University. In coordination with the affected organizational units, the DBRT shall assess and evaluate security incidents and/or personal data breaches, and, in cases of such occurrences, shall be tasked to restore integrity to data processing systems and facilities, mitigate and remedy any resulting damages, and ensure the University's compliance with the reporting requirements of the DPA, NPC Circular 16-03, and other issuances of the NPC pertaining to personal data breach management.

The contact details of the DPO, the ADPO, and the members of the DPC, the DPRT, and the DBRT are found in Part IX of this Manual.

IV. GENERAL DATA PRIVACY PRINCIPLES

The University's processing of personal data shall be conducted in compliance with the following general data privacy principles:

A. *Transparency*. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data by the University, including the risks and safeguards involved, the identities of the persons and offices involved in the processing, his or her rights as a data subject, and how these rights 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 personal data by the University 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 personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed by the University only if the purpose of the processing could not reasonably be fulfilled by other means.

V. RIGHTS OF THE DATA SUBJECT

Pursuant to the provisions of the DPA, data subjects are accorded the following rights, in connection with the processing of their personal data:

A. *Right to be Informed*

The data subject has the right to be informed whether his or her personal data shall be, are being, or have been processed. The data subject shall be notified and furnished with the following information before the entry of his or her personal data into the data processing systems of the University:

- description of the personal data to be entered into the system;
- purposes for which the personal data are being or will be processed, which should be in accordance with the legitimate purposes as stated in Part IV of this Manual;
- 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 or

shared;
- methods utilized for automated access, if the same is allowed by the data subject, the extent to which such access is authorized, and the foreseen consequences of such processing for the data subject;
- the period for which the personal data will be stored;
- the identity and contact details of the DPO; and,
- the existence of his or her rights as a data subject, and how such rights may be exercised.

If, for some valid reasons, the data subject is not notified prior to the entry of his or her personal data into the records of the University, he or she shall be notified at the next practical opportunity.

B. *Right to Object*

The data subject has the right to object to the processing of his or her personal data. In case there are changes to the information given to the data subject as stated in Item (A) above, the data subject shall also be notified and given an opportunity to withhold consent to the processing.

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

- the personal data is needed pursuant to a subpoena;
- the processing is 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 University and the data subject;
- the personal data is being processed to comply with a legal obligation; or,
- there is legal basis for the processing of the personal data.

C. *Right to Access*

The data subject has the right to demand reasonable access to the following:

- contents of his or her personal data that were processed;
- sources from which the personal data were obtained;
- names and addresses of recipients of the personal data;
- manner by which his or her personal data were processed;
- reasons for the disclosure of the personal data to recipients, if any;
- information on automated processes where the personal data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
- date when personal data concerning the data subject were last accessed and modified; and,
- the designation, name or identity, and address of the DPO.

This right, however, does not authorize the data subject to inquire into all records of the University, especially those that are deemed by the University as strictly confidential.

D. *Right to Rectification*

The data subject has the right to dispute inaccuracies or rectify errors in his or her personal data, and the University shall correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the University shall ensure the accessibility of both the new and the retracted personal data and the simultaneous receipt of the new

and the retracted personal data 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.

All University organizational units must take reasonable steps to ensure that the personal information collected or processed are verified, up-to-date, complete, and relevant. The information collected from students is verified by University Registrar's Office, the Office of Student Affairs, and the various Dean's/Principal's Offices. Employee information is verified by the Human Resources Department. In the event of inaccuracy in the information, the data subject concerned may avail himself or herself of the right of rectification.

E. *Right to Erasure or Blocking*

The data subject has the right to suspend, withdraw, or order the blocking, removal, or destruction of his or her personal data from the University's data processing systems.

The exercise of this right may be done 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 purposes 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 by the University;
- the personal data concerns private information that is prejudicial to the data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
- the processing is unlawful; or,
- the data subject's rights have been violated.

The DPO shall notify third parties who have previously received such processed personal data that the data subject has withdrawn his or her consent to the processing thereof.

F. *Right to Indemnification*

The data subject shall be indemnified for any damages actually sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of his or her personal data, taking into consideration any violation of his or her rights and freedoms as a data subject. It shall be the duty of the data subject to prove the damages claimed. The person responsible shall be administratively liable depending on the violation committed. Claims for civil damages may be brought before the NPC or the appropriate courts.

G. *Right to Data Portability*

The data subject has the right to obtain from the University a copy of his or her personal data for his or her further use, where the personal data is processed by electronic means and is in a structured and commonly used format. The exercise of this right shall primarily take into consideration the right of data subject to have control over his or 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.

Transmissibility of Rights of Data Subjects

The lawful heirs and assigns of the data subject may invoke the rights of the data subject to which he or 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 his or her rights.

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.

VI. SECURITY OF PERSONAL DATA

The University shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data in its custody. These security measures are intended to maintain the confidentiality, integrity, and availability of personal data, and protect the same against natural dangers such as accidental loss or destruction, as well as human dangers such as unauthorized access or disclosure, fraudulent misuse, unlawful alteration or destruction, and other unlawful processing.

A. *Organizational Security Measures*

The University's processing of personal data shall adhere to the following guidelines for organizational security:

- The University shall designate accountable personnel for ensuring its compliance with the provisions of the DPA and other applicable laws and regulations for the protection of data privacy and security, and shall communicate the details of such designations to all concerned University stakeholders.
- The University shall implement data protection policies that take into consideration the nature, scope, context, and purposes of the processing of personal data, as well as the risks posed by such processing to the rights and freedoms of its data subjects. The policies shall incorporate the general data privacy principles both at the time of the determination of the means for processing and at the time of the processing itself. These policies shall include, among others:
    - procedures for the collection of personal data, including those for obtaining the consent of data subjects, when applicable;
    - procedures that limit the processing of personal data to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose, including determination of the amount and nature of personal data collected, the nature and extent of the processing involved, the accessibility and/or means of access to the personal data, the nature and period of the data storage and retention, and the conditions and manner of erasure or disposal of the personal data;
    - procedures for data subjects to exercise their rights; and,

- procedures and protocols to follow in case of the occurrence of security incidents or personal data breaches.

The data protection policies shall provide for the documentation, regular review, evaluation, and timely revisions of such policies, as well as the dissemination of the same to all concerned University stakeholders.

- The University shall maintain records that sufficiently describe its data processing systems and identify the duties and responsibilities of the University personnel who will have access to personal data. These records shall include the following:
  - information about the purposes of the processing of personal data, including any intended future processing or data sharing;
  - descriptions of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing;
  - general information about the data flow within the University, from the time of collection, processing, and retention, including the time limits for the disposal or erasure of personal data;
  - general descriptions of the organizational, physical, and technical security measures in place; and,
  - names and contact details of the University personnel accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security.
- The University shall be responsible for the selection and supervision of its personnel who will have access to, or be involved in the processing of, personal data, and shall ensure that these personnel shall operate and hold personal data under strict confidentiality if the personal data are not intended for public disclosure, even upon the transfer of such personnel to other positions or the termination of their employment or contractual relations with SLU. The University shall provide capacity building, orientation, or training programs for such personnel regarding privacy or security policies and best practices.
- The University, through appropriate contractual agreements, shall ensure that its personal information processors, where applicable, shall also implement the provisions of this Manual, and shall only engage personal information processors that provide sufficient guarantees to implement appropriate security measures that ensure the protection of the data privacy rights of data subjects.

B. *Physical Security Measures*

The University's processing of personal data shall adhere to following guidelines for physical security:

- Policies and procedures shall be implemented to monitor and limit the activities in, and access to, the University's data processing facilities.
  - The design and layout of office spaces and workstations, including the physical arrangement of furniture and data processing equipment, shall provide reasonable privacy to personnel who are processing personal data.
  - The duties, responsibilities, and schedules of personnel involved in the processing of personal data shall be clearly defined to ensure that only authorized personnel performing official duties are in the data processing facilities and have access to personal data at any given time. Each unit shall maintain a log of who obtains access to personal data and data processing facilities, and the record keeper shall ensure

that only those with legitimate purpose shall be allowed to gain access, with the purpose also indicated in the log being maintained.

- Policies and procedures shall be implemented regarding the appropriate handling, storage, transfer, removal, disposal, and reuse of removable and electronic media that contain personal data. Hard copies of documents containing personal data shall be stored in secure storage facilities which can be accessed only by authorized personnel, and these storage areas shall be subject to constant monitoring by security personnel.
- Policies and procedures that prevent the mechanical destruction of data files and data processing equipment shall be established. The University's data processing facilities shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

Concerns for the appropriate implementation of physical security measures may be coordinated by the various University units with the Campus Planning, Maintenance, and Security Department, in consultation with the DPC.

C. *Technical Security Measures*

The University's processing of personal data shall adhere to the following guidelines for technical security:

- The University shall implement a security policy with respect to the electronic processing of personal data, which shall provide for the following requirements, among others:
    - safeguards to protect the University's computer network and data processing systems 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;
    - ability to ensure and maintain the confidentiality, integrity, availability, and resilience of the University's data processing systems and services;
    - regular monitoring for security breaches, and a process for identifying and assessing reasonably foreseeable vulnerabilities in the University's computer network and data processing systems, and for taking preventive, corrective, and mitigating actions against security incidents that can lead to a personal data breach;
    - ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    - process for regularly testing, assessing, and evaluating the effectiveness of security measures; and,
    - encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access thereto.

The Technology Management and Development Department, in consultation with the DPC, shall continuously develop and evaluate the University's security policy in connection with the processing of personal data.

VII. MOPG FOR DATA PROCESSING AND PRIVACY POLICIES

All employees, agents, and representatives of SLU are required to strictly respect and uphold the data privacy rights of its data subjects. Failure to observe these rights shall subject the concerned personnel

to possible sanctions. All units in SLU are therefore mandated to afford data subjects these rights in their respective Manual of Operating Procedures and Guidelines (MOPG) on Data Processing and their Privacy Policy.

While this Manual shall govern the data privacy concerns within the entire University, each unit in the University shall have its own MOPG for Data Processing, which shall contain the unit's Privacy Policy. The same shall first be approved by the University President upon favorable recommendation from the DPC. The MOPG on Data Processing and the Privacy Policy shall address the various privacy concerns involving the unit. To ensure that the rights of data subjects are always observed within the entire University, all units should ensure that their MOPG for Data Processing and Privacy Policy should be compliant with this Manual.

It shall be the responsibility of the unit's Head of Office to formulate the unit's MOPG for Data Processing and Privacy Policy. Although the proper implementation of the MOPG, the Privacy Policy, and of this Manual rests upon the entire SLU community, it shall be the Head of Office's ultimate responsibility to ensure faithful compliance with the same by all members of the unit. The Department Heads and the immediate supervisors, being at the forefront of monitoring performance of the faculty members and staff under their supervision, likewise carry the responsibility of making sure that they comply with the provisions of the DPA, this Manual, the unit's MOPG, and the various Privacy Policies that are issued.

The MOPG for Data Processing and the Privacy Policy shall be guided by the following:

A. *What information is collected, stored and retained*
   - All units should ensure that they collect and process only the information which are absolutely needed to be known; hence, over-collection of information should be avoided.
   - Personal Information shall not be collected in anticipation that it may be useful in the future.
   - There must be a statement that authorized university personnel shall collect personal information which is reasonably necessary or directly related to the University's functions or activities or legitimate interests.

B. *What is the purpose of the collection and how is the information used*
   - The purpose should be specific and they may be numerous.
   - While there may be a statement that information shall be used as may be permitted or required by law to pursue SLU's interests as an educational institution which include a variety of academic, administrative, historical and statistical purposes, still, the specific legitimate purposes should be identified.

C. *Who has access to and who processes the information*
   - Only authorized personnel are allowed to access and process the personal information collected from data subjects, and these authorized personnel shall be identified (state functions and not the names of the current holder of the position).
   - Each unit shall develop and implement policies and procedures for the University to monitor and limit access to, and activities in, the units where personal data is processed.
   - For electronic media, the Technology Management and Development Department shall come up with mechanisms concerning its proper use and access.

D. *To whom is the information shared*

- "Data sharing" is the disclosure or transfer to a third party of personal data under the custody of the University or its units. This includes sharing of data to the public through the posting of notices or publications, or the sharing of information to others (parents, guardians, relatives, other academic institutions, researchers, government offices, and many others).
- As a general rule, no University personnel is allowed to disclose personal data unless it is for institutional purposes in line with University policy. The policy shall prevent disclosure to a third party (including a concerned parent) unless written consent has been obtained from the data subject.
- The University shall never share any personal information for commercial purposes.

E. *How long is the information retained and the manner by which the data is disposed*
   - Subject to applicable requirements of the DPA and other relevant laws and regulations, personal data shall not be retained by the University for a period longer than necessary or disproportionate to the purposes for which such data was collected.
   - Do note, however, that under the provisions of the MORPHE and existing Labor Laws, the University is required to permanently keep the student and employee records including the information contained therein. Thus, no personal information may be destroyed unless allowed by such laws, and such destruction, if allowed or authorized by law and the University, must be documented in writing by the University. Unauthorized destruction should be immediately reported to the DPO.

F. *A statement of the rights of the data subject and how they could enforce such rights, and the mechanism of how data breach is handled by the University*
   - As this mechanism is already provided in detail in this Manual, the Privacy Policy may simply incorporate the provisions of this Manual by way of reference.

G. *A mechanism of obtaining the consent of the data subject*
   - When required by the DPA or other applicable laws or regulations, the consent of the data subjects should be properly obtained and must be evidenced by written, electronic, or recorded means.
   - This may be done by indicating in the various data collection and processing forms a statement that the data subject is allowing SLU to collect, use and process his or her personal data where a legitimate educational or institutional interest exists in SLU's determination, as enumerated in its Privacy Policies.

H. *A statement of the existence of this Manual and that the data subjects may refer to this document to know more about the details concerning their right to privacy vis-à-vis SLU's legitimate interests.*

Common data privacy issues shall be the subject of a uniform Privacy Policy.

- For *student-related* University-wide data privacy concerns, there shall be a *Student Privacy Policy* applicable to the applicants for admission, existing students, as well as the alumni. The formulation, review, and revision of the said policy shall be the collective responsibility of the Office of Student Affairs, the Registrar's Office, the Guidance Center, and the various Schools. For administrative purposes, the Office of Student Affairs shall take the lead with respect to all matters involving the Student Privacy Policy.
- For *employee-related* University-wide privacy concerns, there shall be an *Employee Privacy Policy*. The formulation, review, and revision of the said policy shall be the collective responsibility of the

Human Resources Department, in coordination with all Schools and offices. For administrative purposes, the Human Resources Department shall take the lead with respect to all matters involving the Employee Privacy Policy.

- For other common privacy matters, the unit that is directly and regularly interacting with the data subject shall take the lead in coming up with the Privacy Policy. Smaller units with similar privacy concerns like the University Clinics and Residence Halls may likewise come up with a common Privacy Policy.

Within ninety (90) days from effectivity of this Manual, all units within the University should come up with their respective MOPG for Data Processing. The MOPG shall be submitted to the DPC for review and appropriate action.

VIII. DATA BREACH AND SECURITY INCIDENTS

It shall be a fundamental policy that, in the case of security incidents or personal data breaches, immediate action must be taken, even if the same is a mere suspicion and even if the extent of the breach has not yet been determined.

It shall be the duty of all employees, agents, and representatives of the University involved in the processing of personal data to regularly monitor for signs of possible security incidents or personal data breaches. In the event that such signs are discovered, or when there is reasonable belief that a security incident or personal data breach has occurred, the facts and circumstances regarding the same shall be immediately reported to the Head of Office, who, in turn, shall immediately report the matter to the DPO for verification.

If the DPO has ascertained that there is a likelihood that a personal data breach has indeed occurred, the DPO shall convene the DBRT, which shall determine whether or not a personal data breach requiring notification under the DPA has occurred, and the relevant circumstances surrounding the reported security incident or personal data breach. If required by the circumstances, the DPO shall notify the NPC and the affected data subjects pursuant to the requirements and procedures prescribed by the DPA.

The notification to the NPC and the affected data subjects shall at least describe the nature of the breach, the personal data possibly involved, and the measures taken by the University to address the breach. The notification shall also include measures taken to reduce the harm or negative consequences of the breach to the data subjects, as well as and the name and contact details of the DPO. The form and procedure for notification shall conform to the regulations and circulars issued by the NPC, as may be updated from time to time.

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 University. 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 by the DPO to the NPC annually.

IX. INQUIRY ON DATA PRIVACY ISSUES AND CONCERNS

The University's data subjects may inquire or request for information from any member of the DPC or the DPRT regarding any matter relating to the processing of their personal data under the custody of SLU, including the data privacy and security policies implemented to ensure the protection of their personal data.

Inquiries may be coursed through any of the following:

Data Protection Committee:

The Vice President for Administration/Data Protection Officer
Ground Floor, SLU Administrative Center (Local 322)
privacy@slu.edu.ph

The Assistant Data Protection Officer
c/o ICT Research Laboratory
SLU Maryheights Campus (442-6321 local 216)

The Director, Campus Planning, Maintenance, and Security Department
2nd Floor, Diego Silang Building (Local 376)

Inquiries involving specific matters may also be coursed through:

The Director, Human Resources Department
Second Floor, SLU Administrative Center (Local 285)

The Vice President for Finance
Second Floor, Diego Silang Building (Local 217)

The Director, Technology Management and Development Department
1st Floor, Diego Silang Building (Local 390)

The University Registrar
Second Floor, Diego Silang Building (Local 213)

The Dean, Office of Student Affairs
2nd Floor, Diego Silang Building (Local 321)

The Registrar, SLU-LES
SLU General Luna Campus (442-6883 local 104)

The Registrar, SLU-LHS (Junior and Senior High)
SLU Navy Base Campus (442-2648)

The Legal Affairs Director
Ground Floor, SLU Administrative Center (Local 247)

X. REVIEW OF DATA PRIVACY POLICIES AND PROCEDURES

The DPO and the ADPO, in consultation with the appropriate units in the University, shall ensure that all policies and procedures in connection with data privacy are updated, and that such policies and procedures are implemented, monitored, reviewed, evaluated, and revised as may be needed to ensure that the rights of the data subjects are respected, and that the processing of personal data is done fully in accordance with the DPA and all applicable laws and regulations in relation to education and privacy.

XI. EFFECTIVITY

This 2019 Edition of the Data Privacy Manual shall take effect upon approval by the University President, and shall supersede the SLU Data Privacy Manual of 2017.