Data Privacy Manual

Classification: Administration and Operations
Approval Authority: Office of the Chancellor
Implementation Authority: Data Privacy Office
Effective Date: January 25, 2019
Latest Revision: January 25, 2019

Table of Contents

The University's Commitment to Data Privacy

The university is committed to safeguarding the privacy of the individuals that it interacts with on a daily basis as the university conduct its operations to become a leading learner-centered and research University bridging faith and scholarship, attuned to a sustainable Earth, and in the service of Church and society, especially the poor and marginalized. This privacy manual is adopted in compliance with the requirements of RA10173 otherwise known as the Data Privacy Act of 2012.

Purpose of the Manual

All personal data collected by or within the university, processed, transmitted, disclosed, and stored are considered personal data assets. A personal data asset refers to any media in paper or electronic form that contains personal data as defined by RA10173. These assets are to be protected against their compromise in terms of confidentiality, integrity, and availability as well as to ensure that their processing are authorized and compliant with relevant data privacy regulations. This manual aims to assist the university in demonstrating the practice of due care and due diligence in the protection of personal data.

The privacy manual aims to address and seeks to protect personal data in terms of (in compliance with RA 10173);

- Confidentiality – Ensuring the protection of personal data from improper disclosure and use or unauthorized processing. Any unauthorized disclosure and processing of personal data may lead to data breaches that may cause financial and reputational losses to the university.

- Integrity – Ensuring data and processes are protected from improper modification as well as incorrect capture of personal data and inconsistency of maintenance of personal data. Safeguarding the accuracy and completeness to ensure full confidence in the quality of the data should be practiced by the university. Loss of data integrity may lead to data processing based on inaccurate data that may cause the data subjects to file complaints against the university with the National Privacy Commission.

- Availability – Ensuring only authorized access to personal data as well as providing authorized users with immediate and readily available access to the personal data when required. This also requires that corruption and/or loss of data during collection, processing, and storage should be avoided. Loss of data availability or excessive access to personal data may be viewed as improper disposal and unauthorized disclosure. Both of which are punishable acts under RA10173.

Some of the most likely vulnerabilities and threats to personal data based on SANS Institute Threat Landscape Survey and ISO 27001/2:2013 practices;

- Non-compliance with privacy manual, policies, and procedures of people within the organization
- Weakness in monitoring and enforcement of privacy policies and procedures at an organizational, physical, and technical level
- Lack of data management and governance
- Introduction of malware (viruses/worms/ransomware) by people within the organization
- Data Infrastructure intrusions by both internal and external sources
- System application design and implementation flaws
- Disgruntled employees/contractors with malicious intent
- Inappropriate use/abuse of communications facilities (i.e. telephone, fax, messaging, email, Internet),
- Unauthorized access or disclosure of personal data thru negligence, social engineering, phishing emails, chain letters, computer fraud, and utility failures.

To address the above vulnerabilities and threats to personal data, the university implements and maintains a Privacy Management Program as well as implement organizational, physical, and technical controls that are risk based and resource optimized to minimize the organizational risk to an acceptable level and satisfy both the university senior management and the data subjects privacy requirements while overall reducing the impact and costs of any privacy breach.

Definition of Terms

[Source: RA 10173 https://privacy.gov.ph/data-privacy-act/]

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:

1. About an individual, race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. About an individual, 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;
3. 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
4. Specifically established by an executive order or an act of Congress to be kept classified.

Data subject – refers to an individual whose personal, sensitive personal, or privileged information is processed;

Data processing systems - refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;

Data sharing - is 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;

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 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 information controller - refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;
3. There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

Personal information processor - refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;

Processing – refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means or manual processing, if the personal data are contained or are intended to be contained in a filing system;

Profiling - refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

Public authority - refers to any government entity created by the Constitution or law, and vested with law enforcement or regulatory authority and functions;

Incident – refers to an event that violates the university's policy and procedures.

Privacy Incident – refers to suspected or confirmed incident involving personal data. It can include any successful or unsuccessful loss of control, compromise, or unauthorized disclosure, acquisition, access of personal data, and its improper disposal. A Privacy Incident may involve any or all of the following:

- a violation of university privacy policies and standards,
- unauthorized system access,
- loss of personal data confidentiality,
- loss of personal data availability,
- compromise of personal data integrity,
- misuse of service, systems or information with personal data, or
- Physical or logical damage or loss to systems containing personal data

A Privacy Breach – refers to when a privacy incident meets legal definitions that require notification to the affected individuals, regulatory agencies, as well as the National Privacy Commission.

Due Diligence - reasonable steps are taken in order to comply with a legal requirement

Due Care – "Degree of care that an ordinary and reasonable person would normally exercise, over his or her own property or under circumstances like those at issue. The concept of due care is used as a test of liability for negligence". (Business Dictionary)

Scope of the Manual

This privacy manual applies to the general practices on personal data processing within the university, however there may be cases where there is a need to have a slightly different privacy practice. If there will be a different privacy practice it will be made clear that privacy practice differs from this general privacy manual. Also note that the DLSU reserves the right to change, amend and/or vary this manual at any time.

The manual applies to the general personal data collection and processing activities of the DLSU Manila with campuses in Makati, Bonifacio Global City, and Laguna. Each unit or department within the university can define their own supplemental policies, procedures, or manuals upon approval of the Data Privacy Office in order to supplement this document. However, any such definitions shall remain consistent with the overall intentions of this manual. The university policies stated in this manual are mandated and all (i.e. employees, temporary contractors, business partners, and vendors) are responsible to act, and abide by these policies and report any violations.

All authorized employees, consultants, and external third party (vendors, suppliers) with access to university scoped personal data and its processes must comply with the privacy manual.

Data and Document Classification and Management

In order to better manage and comply with privacy regulatory requirements, data and document classification and management shall be put in place to oversee access and processing of personal data.

1. A list of all personal data assets will be stored in the "Personal Data Inventory Register" located within a centrally controlled document repository for managing university resources which shall be reviewed on an annual basis.
2. A Privacy Impact Assessment shall be conducted and maintained with respect to the data inventory in order to develop and maintain an impact assessment register or risk register which is centrally controlled and shall be reviewed on an annual basis.
3. Personal data assets must be classified in accordance with university needs and the impacts associated with those needs. Each department or unit head shall determine and classify the personal created and collected, maintained, stored, disclosed, and disposed; and to identify the authorized personnel and their access privileges (read, write, execute, or any combination) to the personal data. The following levels of classification shall be used and the personal data handled accordingly.

Classification	Description
Sensitive	This generally refers to information that contains or relates to sensitive personal information. This information is private and very sensitive and must be strictly monitored and controlled at all times. Unauthorized access, processing, disclosure, and disposal of this information to people without any legitimate purpose for access could be a violation of the privacy manual as well as the privacy regulatory requirements. Collection, access, processing, disclosure, and disposal of sensitive personal information is restricted, and such access will only be given when a specified legitimate purpose aligned with the original intention of personal data collection has been demonstrated. Collection, access, processing, disclosure, and disposal of sensitive personal information classified as sensitive beyond the stated purpose upon its collection must be approved by the data protection officer. Sensitive Personal Information refers to information: 1. About an individual, race, ethnic origin, marital status, age, color, and religious,

Classification	Description
	philosophical or political affiliations; 2. About an individual, 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; 3. 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 4. Specifically established by an executive order or an act of Congress to be kept classified. Sensitive personal information shall be labelled and classified as "SENSITIVE" for each page and affix a "[SENSITIVE]" watermark or stamp on the cover sheet listing the personal data classification. Data subjects consent shall be acquired before collection and use of such information in accordance with the requirements of RA10173.
Personal Confidential	This information relates to the personal information that must be protected in accordance with the Philippine Data Privacy Principles where access must be restricted to those with a legitimate purpose. Collection, access, processing, disclosure, and disposal to "Personal Confidential" information is restricted, and such access will only be given when a specific legitimate interest has been demonstrated. And such access will only be given when a specified legitimate interest aligned with the original intention of personal data collection has been demonstrated. Examples include: • Data Subjects Name • Biometric Information • Genetic Information • Photo and Video • Mobile Number, Email Addresses, and Physical Addresses that have accompanying data subjects name • Signature All of the above types of information shall be labelled

Classification	Description
	"Personal Confidential" for each page and affix a "[PERSONAL CONFIDENTIAL]" watermark or stamp on the cover sheet listing the personal data classification. Consent shall be collected prior to personal data collection or as soon as practicable and reasonable.
Private Internal	This refers to information not classified as personal data within RA10173 but is intended for use within the university and in some cases within affiliated organizations, such as third-party partners only. Access to "Private Internal" information is restricted by access controls to a broad group of users at department or unit levels. Examples of information classified "Internal" includes: • Organizational information • Communication records • Employment records outside of Personal Data All of the above information shall be labelled with an "[PRIVATE INTERNAL]" watermark or stamp on the cover sheet listing the information security classification.
Public	Any information textual or graphical that has been posted for public access such as in the case of a social media posting as ruled by the Supreme Court or when appropriate informed consent has been collected for the public disclosure of the information.

Key Responsibilities

In order to achieve compliance with privacy regulations and be able to implement this privacy manual, key responsibilities are to be assigned and recognized by the following relevant individuals:

- Board of Trustees – provide general oversight on privacy implementation and compliance. Serves as overall arbiter and final decision maker on privacy initiatives.
- Administrators and Management – Monitoring and assessment of privacy risks is undertaken on a regular basis. Apply relevant university policies and procedures to personal data assets under

their control, and promote commitment for the privacy manual and compliance with RA10173.

- Data Protection Officer – serves as liaison with the National Privacy Commission. Ensure implementation of the privacy management program.
- Faculty and Staff –responsible for protecting the personal data assets of the data subjects related to the university from leakage, loss, failure in terms of integrity, and unauthorized processing. Each employee shall assist in this endeavor by being responsible to be aware of all relevant privacy policies and procedures that deal with the access and processing of personal data starting with the Privacy Manual. The employee is also responsible for reporting immediately any perceived potential violation or threat to the security of the personal data assets directly to their immediate superiors.
- Third-party partners – privacy obligations should be formalized in a contractual agreement, specifying how information will be used, shared, accessed, processed, logged, stored, backed-up, transmitted and/or destroyed.
- Data Subject – take utmost care in safeguarding their privacy rights and exercise due diligence in disclosure of personal data and must not be negligent in protecting their privacy rights.

Annual Reporting

External Reporting – Annual external reporting to the National Privacy Commission is required under the law. The report shall contain summaries of incidents within the year as well as activities taken to ensure compliance with the data privacy act. The format of the report shall follow the template to be issued by the National Privacy Commission.

Internal Reporting – Annual internal reporting shall be conducted to include details of incidents, breaches, compliance activities, internal audits, as well as changes from previous processes. Details shall include information that can be used for analytics purposes to determine trends, hot spots, effectiveness of activities, as well as pending activities not yet accomplished. Proper baselining should also be shown in the reports as well as document control and versioning.

Privacy Policies

Collection of Personal Data

In the collection of personal data, it is important that the principles of Transparency, Legitimate Purpose, and Proportionality be upheld as required by the Data Privacy Act of 2012.

1. Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or 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.(Section 18 RA10173 IRR)

2. Legitimate purpose. The processing of information shall be compatible with the declared and specified purpose which must not be contrary to law, morals, or public policy. (Section 18 RA10173 IRR)

3. Proportionality. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. (Section 18 RA10173 IRR)

In terms of the need to acquire consent in the collection of personal data, the following should be considered before the actual collection:

1. The data subject is of legal or majority age. Any consent collected from minors in not valid in the court of law. Hence, collection of personal data without consent of the legal guardian is not allowed.

2. The collection of consent should be a secondary compliance measure as this requires the management of consent due to the potential of consent withdrawal by the data subject at any point in time in the future. Once consent has been revoked, access and processing of the affected personal data should no longer be allowed.

3. Redundancy of data collection should be discouraged if not disallowed. This refers to repeated collection of personal data from data subjects when they have already been collected in a prior instance. In the creation of multiple copies of personal data, this would exponentially increase the risk of exposure of the university to non-compliance and even cases that may be filed due to non-compliance or breaches by the data subject in the future. It is recommended that processes be put in place that would allow the reduction or prevention of redundant data collection.

4. Collection of personal data that requires consent should have a consent form provided and all responses tracked in a secure manner. Consent statements should state clearly the personal data to be collected, the purpose of personal data collection, the storage policy and procedure for the personal data, the processing to be performed on the personal data collected, any disclosure or sharing of data that would be needed for the stated purpose, and the retention period of the collected personal data.

5. In collecting personal data, the legitimate purpose of collection should be established. Listed below are the reasons for data collection that are considered of legitimate purpose by the Data Privacy Act of 2012.
    a. Personal Information Collection (Section 21 RA10173 IRR)
        i. The data subject must have given his or her consent prior to the collection, or as soon as practicable and reasonable;
        ii. 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;
        iii. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
        iv. The processing is necessary to protect vitally important interests of the data subject, including his or her life and health;
        v. 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;
        vi. The processing of personal information is necessary for the fulfillment of the constitutional or statutory mandate of a public authority; or
        vii. The processing is necessary to pursue the legitimate interests of the personal information controller, 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 Philippine Constitution.

    b. Sensitive personal information Collection (Section 22 RA10173 IRR)
        i. 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;
        ii. 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;
        iii. 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 or her consent prior to the processing;
        iv. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations provided that:
            1. Processing is confined and related to the bona fide members of these organizations or their associations;

2. The sensitive personal information are not transferred to third parties; and
3. Consent of the data subject was obtained prior to processing;

v. 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

vi. 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

6. When collecting consent from the data subject, implied and generic consent statements are not allowed by law as stated in Section 3 of the RA10173 IRR. It states that
   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 his or her personal, sensitive personal, or privileged information.
   b. 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;
   c. It can also be seen from the **NPC Advisory Opinion 2017-42** (https://privacy.gov.ph/wp-content/files/attachments/advopn/NPC AdvisoryOpinionNo. 2017-042.pdf) that implied or generic consent is not allowed.

7. With respect to employer-employee relations, please refer to **NPC Advisory Opinion 2017-50 and 2017-51** (https://privacy.gov.ph/wp-content/files/attachments/advopn/NPC AdvisoryOpinionNo. 2017-050.pdf, https://privacy.gov.ph/wp-content/files/attachments/advopn/NPC AdvisoryOpinionNo. 2017-051.pdf. Relevant excerpts are as follows:
   a. With regard to the phrase "but not limited to," its inclusion in the employment contract does not mean that such stipulations amount to blanket consent. An elementary rule in statutory construction provides that when general words accompany an enumeration of particular cases, such words only apply to cases of the same kind as those expressly mentioned.1 For instance, "work-related requirements" in the employment contract should refer to those having the same purposes as those enumerated, i.e., it should be work-related. It does not amount to the data subject consenting to the use of their personal information for any and all purposes.
   b. A Personal Information Controller (PIC), such as your employer, can also process personal information when it is necessary and is related to the fulfillment of a contract with the data subject,3 such as a contract for employment. This would include

computation and payment of salaries and other benefits, determination of career movements, facilitation of work-related requirements, and outsourcing of human resource management functions.

c. Another instance is when the processing of personal information is necessary for compliance with a legal obligation to which the personal information controller is subject and when processing is provided for by existing laws and regulations. This would include compliance with statutory and regulatory requirements of national government agencies, to which the employer is subject to.
d. In fact, consent in the abovementioned instances may not even required by the DPA, since the processing would fall under another criteria for lawful processing.
e. However, with regard to processing of sensitive personal information, consent of employees is required unless processing falls under any of the other instances provided in Section 13. When personal data of employees is used for marketing purposes, consent is required as this is neither necessary nor related to an employer-employee contract. If consent cannot be obtained, the employer should avoid using personal information for marketing purposes.

Data Collection for Students

Applicant/Student - Personal Data which includes name, nick name, address (permanent and current), date of birth, country of birth, country of citizenship, gender, contact information (e.g. telephone number, mobile number and email address), last high school attended, senior high school track, application fee information, proof of citizenship, religious philosophical political affiliations, previous academic standing (Form 137), personal declaration/s pertaining to physical/behavioral/disciplinary conditions and degree program/s applying for. Upon successful admission and enrollment, the university collects personal data with regards to academic performance and activities.

Upon enrollment – Personal Data which includes name, nick name, address (permanent and current), date of birth, country of birth, country of citizenship, gender, contact information (e.g. telephone number, mobile number and email address), last high school attended, senior high school track, application fee information, proof of citizenship, religious philosophical political affiliations, previous academic standing (Form 137), personal declaration/s pertaining to physical/behavioral/disciplinary conditions and degree program/s applying for.

During your stay as a student – the university regularly collects personal data such as academic performance and activities, annual physical checkups or medical and health related tests, performance evaluations, potential administrative or legal cases, philosophical affiliations such as memberships to fraternities and related information, photos and videos directly taken such as in cases of official activities or indirectly taken such as the case of group or scene photos and videos or videos taken as a result of the use of closed-circuit cameras.

Upon Graduation – the university collects and generates information such as but not limited to diploma and transcript of records that provide details about educational performance and attainment that is to be kept by the university for record purposes.

Data Collection for Faculty

Prior to employment - Personal Data which includes name, nick name, address (permanent and current), date of birth, country of birth, country of citizenship, gender, contact information (e.g. telephone number, mobile number and email address), educational background, professional affiliations or certifications, religious philosophical political affiliations, information on previous employment, medical and health related documents and declarations.

Upon acceptance - the university collects personal data with regards to work performance and activities as well as documents needed to process the application for employment status. The personal data collected includes personal information as written in the personal data sheet which includes a photograph of the applicant, government issued identifications such as those given by the BIR, SSS, PAG-IBIG, and PhilHealth, government issued clearances such as barangay clearance, police clearance, and NBI clearances, government certifications such as birth and marriage certificates, medical and health related clearances, and bank account details for processing of compensation.

During employment – the university regularly collects personal data such as annual physical checkups or medical and health related tests and benefit claims, performance evaluations, potential administrative or legal cases, philosophical affiliations such as memberships to unions and related information, photos and videos directly taken such as in cases of official activities or indirectly taken such as the case of group or scene photos and videos or videos taken as a result of the use of closed-circuit cameras. The university also collects information about academic, professional, and research related activities, awards and outputs as needed for the legitimate interest of the university.

Data Collection of CAP Data

Prior to employment - Personal Data which includes name, nick name, address (permanent and current), date of birth, country of birth, country of citizenship, gender, contact information (e.g. telephone number, mobile number and email address), educational background, professional affiliations or certifications, religious philosophical political affiliations, information on previous employment, medical and health related documents and declarations.

Upon acceptance - the university collects personal data with regards to work performance and activities as well as documents needed to process the application for employment status. The personal data collect includes personal information as written in the personal data sheet which includes a photograph of the applicant, government issued identifications such as those given by the BIR, SSS, PAG-IBIG, and PhilHealth, government issued

clearances such as barangay clearance, police clearance, and NBI clearances, government certifications such as birth and marriage certificates, medical and health related clearances, and bank account details for processing of compensation.

During employment – the university regularly collects personal data such as annual physical checkups or medical and health related tests and benefit claims, performance evaluations, potential administrative or legal cases, philosophical affiliations such as memberships to unions and related information, photos and videos directly taken such as in cases of official activities or indirectly taken such as the case of group or scene photos and videos or videos taken as a result of the use of closed-circuit cameras.

Data Collection of Legal Guardian

Legal Guardian - Personal Data which includes name, address, contact information (e.g. telephone number, mobile number and email address). Government Issued IDs that are classified as sensitive personal information.

Legal Guardian of Scholar Applicant/Student - Personal Data same as that of the Legal Guardian, proof of financial standing that includes utilities billing statements, bank or credit card statements, and similar proofs of financial standing. Although financial data is considered confidential and not under the data privacy act, such documents often contain personal data in the form of personal information that can be used to identify or cause harm to the data subject.

Data Collection of Visitors to the University

When you enter our campus as a visitor or guest, the university collect your personal data such as a valid ID (e.g. drivers license, company ID) which is deposited with an authorized security personnel and replaced temporarily with a visitor pass. If the visitor is driving a vehicle, the plate number of the vehicle will be recorded. The visitor will be asked to sign a logbook that states their identity and purpose of visit to our campus. As you walk around the campus, CCTV cameras will be recording the visitors presence at various key locations of the campus as well as its entry and exit points. For website visitors please refer to our privacy policy as published in our website.(https://www.dlsu.edu.ph/privacy/)

Objection to Collection

All data subjects have the right to object to personal data collection and processing. Consent given previously can also be withdrawn at any time when the data subject deems it necessary considering for a fact that revoking consent or exercising the right to object when it contradicts the needs of a legitimate purpose such as a contractual obligation with the data subject may interfere with the successful and smooth implementation of the contract. If such is the case, the request of the data subject may not be approved. Objections raised by data subjects should be sent to the Data Privacy Office then disseminated and enforced accordingly with the unit involved.

Use of Personal Information

The acceptable collection and use or processing of personal data is based on the stated purpose upon point of collection. Blanket consent is not allowed even if some generic terminologies may be used. Upon use of generic terminologies, it is assumed that the use is only applied to the same kind of as those expressly mentioned. Any deviation from the stated purpose should require a separate consent to be acquired from the data subject unless it falls under the legitimate use or exceptions as provided by the law **(Section 5, 21, 22 of the RA10173 IRR).** Exception excerpts are as follows **(from Section 5 of RA10173 IRR):**

- Information processed for purpose of allowing public access to information that fall within matters of public concern
- 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
- 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;
- 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.
- 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.

Declared Purpose for Processing Student Data

The personal data collected about the students in the university is used and processed in the following manner:

- Verification process for taking the admissions examination
- Information dissemination by the university with respect admissions and its programs
- Protection of the health and vital interest of the applicant/student thru medical or health evaluation
- Preparation processes for ceremonial activities such as orientation events of the various programs and colleges
- Determining the enrollment status of the applicant
- Processing of grants or documents needed in partnerships that the university will undertake
- Setting up or processing needed in academic systems such as Learning Management Systems, Electronic Libraries, Uniform distribution systems
- Internal process improvement activities that may include the use of data analytics to process the personal data
- Use in religious practices as supported and sanctioned by the university

- Use in emergency situations to protect the vital and medical interest of the applicant/student

Declared Purpose for Processing Faculty Data

The personal data collected about the employee is used and processed in the following manner:

- Validation and identification of the applicant / employee
- Employment assessment and evaluation
- Verification process such as background checks, credit checks, educational attainment verification
- Lawful non-commercial information dissemination by the university with respect to its legitimate interests
- Protection of the health and vital interest of the applicant/student thru medical or health evaluation and activities
- Processing of administrative tasks such as payroll processes, benefits processing, performance evaluations, disciplinary actions, and other administrative tasks
- Processing of grants or documents needed in partnerships that the university will undertake
- Setting up or processing needed in university information systems such as HRIS.
- Internal process improvement activities that may include the use of data analytics to process the personal data
- Use in religious practices as supported and sanctioned by the university
- Use in emergency situations to protect the vital and medical interests of the applicant/employee

Declare Purpose for Processing CAP Data

The personal data collected about the applicant/employee is used and processed in the following manner:

- Validation and identification of the applicant / employee
- Employment assessment and evaluation
- Verification process such as background checks, credit checks, educational attainment verification
- Lawful non-commercial information dissemination by the university with respect to its legitimate interests
- Protection of the health and vital interest of the applicant/student thru medical or health evaluation and activities
- Processing of administrative tasks such as payroll processes, benefits processing, performance evaluations, disciplinary actions, and other administrative tasks
- Setting up or processing needed in university information systems such as HRIS.
- Internal process improvement activities that may include the use of data analytics to process the personal data
- Use in religious practices as supported and sanctioned by the university

- Use in emergency situations to protect the vital and medical interests of the applicant/employee

Declared Purpose for Processing Student Scholar Data

The personal data collected about the scholar applicant/student is used and process in the following manner:

- All processes of an applicant/student.
- Search for volunteers by various colleges and departments

Declared Purpose for Processing Legal Guardian Data

The personal data collected about the Legal Guardian is used and processed in the following manner:

- Use in emergency situations to protect the vital and medical interests of the applicant/student

Declared Purpose for Processing Student Scholar Legal Guardian Data

The personal data collected about the Legal Guardian of Scholar Applicant/Student is used and processed in the following manner:

- All processes of a Legal Guardian.
- Used in conjunction with financial related documents to determine the qualification to the scholarship program

Declared Purpose for processing personal data of visitors

The university collects personal data as part of its security procedure to ensure the safety of the people within the campus as well as to serve as aide for possible investigations on violations to University policies and any applicable laws and regulations. The personal data may also be used to generate aggregate statistical reports as input to improve university processes and services.

Access to Personal Data

Access to personal data collected by the university shall be allowed and the request to access shall be channeled thru the appropriate unit who collected and maintains the personal data (e.g. University Registrar for personal data related to enrollment). However, access to documents containing the data subjects personal data that includes personal data of other data subjects not included in the request shall only be allowed when the consent of all related data subjects have been acquired or if it is in compliance with a legal requirement of that or a requirement of a public authority. This is to ensure that the rights of all data subjects are protected under the supervision of the university.

Keeping Data Subject Informed

Data subjects have the right to be informed with regards to the processing of their personal data as well as possible breaches to the access and processing of their personal data. Data subjects shall be informed when the processing of their personal data goes beyond the originally stated purposes or consent previously acquired unless otherwise allowed within the special cases or exemptions within the Data Privacy Act and its corresponding IRR. In the event of an incident or a breach, policies and procedures will follow the Incident and Breach Management Plan. Notification of the data subject shall be performed in compliance with the requirements under the law specifically "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 personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject." (Section 38 RA10173 IRR)

Sharing of Personal Data

Sharing of personal data within the university shall follow the principles of Transparency, Legitimate Purpose, and Proportionality. Personal data collected for a specific processing purpose shall not be shared with other units within the university unless the data subject was notified during collection of the intention to share the data (Transparency), processing purpose adheres to the stated purpose during data collection even if used by another unit and following the requirements of legitimate purpose, and shall state clearly the rationale for the specific types or fields of data to be shared whereby the rationale shall not conflict with the rights of the data subject and does not exceed the minimum amount of data needed for the stated rationale (Proportionality).

Sharing of Student Data

The personal data of both the students are shared with the following units within the university for the previously stated purposes:

- Colleges, Departments, University Administrators, and Scholarship Donors of the university relevant to the degree program of the applicant/student
- ITEO for exam and evaluation purposes as well as for conducting internal improvement surveys and research
- University Clinic for medical or health related requirements
- OCCS for counseling and career related activities
- University Library for monitoring of library usage
- University Security and Discipline office for maintaining security to the university
- Accrediting agencies or organizations that the university seeks to be accredited to or participate in.

- Other universities, organizations, government agencies, that the university seeks to partner, collaborate or apply for grants to.
- Public information dissemination in cases where the student is being recognized by the university or other organizations as well as in cases where personal data of the student is directly a participant of and is needed for publication of academic and research works.
- Aggregated data may be generated from personal data for study and reporting purposes
- Parents or Legal Guardian of the applicant/student for information purposes
- Upon graduation, collected and processed data shall be shared with the Advancement and Alumni Relations Office for management of alumni activities.
- Personal Data SHALL NOT be shared with parties not currently stated without prior additional consent from the data subject

Sharing of Faculty Data

The personal data of both the applicant/employee are shared with the following units within and external to the university for the previously stated purposes

- Colleges and Departments relevant to the position currently held by the employee or is being applied for by the applicant
- Government agencies where mandatory reporting is required such as BIR, SSS, PAG-IBIG, PhilHealth, DOLE.
- University Clinic for medical or health related requirements
- University Library for monitoring of library usage
- University Security and Discipline office for maintaining security to the university
- Accrediting agencies or organizations that the university seeks to be accredited to or participate in.
- Other universities, organizations, government agencies, that the university seeks to partner, collaborate or apply for grants to.
- Public information dissemination in cases where the faculty is being recognized by the university or other organizations as well as in cases where personal data of the faculty is directly a participant of and is needed for publication of academic and research works.
- Third party contractors or service providers duly vetted by the university for lawful non-commercial use serving the legitimate interest of the university
- Employment information requests by prospective organizations that the employee is transferring to or applying for.
- Aggregated data may be generated from personal data for study and reporting purposes
- Personal Data SHALL NOT be shared with parties not currently stated without prior additional consent from the data subject

Sharing of CAP Data

The personal data of both the applicant/employee are shared with the following units within and external to the university for the previously stated purposes

- Colleges and Departments relevant to the position currently held by the employee or is being applied for by the applicant
- Government agencies where mandatory reporting is required such as BIR, SSS, PAG-IBIG, PhilHealth, DOLE.
- University Clinic for medical or health related requirements
- University Library for monitoring of library usage
- University Security and Discipline office for maintaining security to the university
- Accrediting agencies or organizations that the university seeks to be accredited to or participate in.
- Third party contractors or service providers duly vetted by the university for lawful non-commercial use serving the legitimate interest of the university
- Employment information requests by prospective organizations that the employee is transferring to or applying for.
- Aggregated data may be generated from personal data for study and reporting purposes
- Personal Data SHALL NOT be shared with parties not currently stated without prior additional consent from the data subject

Sharing of Legal Guardian Data

The personal data of the legal guardian are shared with the following units within the university for the previously stated purposes

- Colleges and Departments relevant to the program or degree of the applicant/student
- ITEO for exam and evaluation purposes as well as for conducting internal improvement surveys and research
- University Security and Discipline office for maintaining security to the university
- Aggregated data may be generated from personal data for study and reporting purposes
- Applicant/Student for information purposes
- Personal Data SHALL NOT be shared with parties not currently stated without prior additional consent from the data subject

Disclosure of Personal data to accrediting agencies and organizations

In disclosing or sharing personal data with accrediting agencies such as PAASCU, AUN, and auditing firms or with organizations such as UAAP, PUSO, DLSAA, proper data sharing agreement should be executed with such organizations unless data disclosed remains within the premises of the university and is not copied to an external destination. In cases when data is not copied or disclosed outside of the university premises, a non-disclosure agreement shall be executed with those who can view the personal data within the university.

Disclosure of Personal data to third party vendors or partners

When entering into contracts with third party service providers, vendors, and partners, unless the disclosure is already covered by existing consent statements and data sharing agreements, all contracts should be sent to the Data Privacy Office for approval prior to entering into the contract.

Disclosure of Personal data on Social Media Platforms

Posting personal data on social media should not be performed without the prior acquisition of the consent of the data subject. Even upon acquisition of the consent of the data subject, personal data posted should be kept to a minimum based on the needed purpose. Posting of personal data of multiple data subjects on social media for official purpose of the university should be reviewed by the Data Privacy Office prior to its publication.

Posting on social media on a personal capacity is not within the scope of the Data Privacy Act.

Maintenance of Accuracy of Personal Data

Aside from the exercise of due care and due diligence in the collection and processing of personal data during its normal course of use, the data subject can exercise their right to the correction of inaccurate personal data collected and maintained by the university. In exercising such right, the data subject shall first raise their concern to the unit involved to request for correction of the personal data stored. The Data privacy office shall be given a monthly report of all correction requests by each unit duly certified by their unit heads in terms of the integrity of the report. This shall serve as a record of compliance to the Data Privacy Act. In the event that there is ambiguity in the process of correcting personal data, the data subject may directly contact the Data Privacy Office with regards to their concern for proper routing of request.

Personal Data Storage

The personal data of all data subjects in DLSU are stored in the following manner:

- The physical document collected are stored under lock and key in secure storage locations such as steel cabinets and can only be opened by authorized personnel.
- The electronic version of the personal data whether digitized or transcribed are stored in university information systems that are housed within the university premises mostly with some information stored externally with service providers for efficiency as well as for business continuity purposes. Only authorized personnel are given the rights to access the data thru various access control mechanisms.
- Storing of personal data collected by the university on personal devices (e.g. flash drives, memory cards, laptops) and personal cloud services (e.g. Gmail, Google Drive, OneDrive, DropBox) is not allowed.

Personal data should be stored under university provided accounts using the DLSU.EDU.PH domain or university provided equipment.

- Whenever possible or feasible, encryption should be employed on personal data at rest specially if such personal data shall be brought outside of the campus.
- Personal Data shall not be stored in shared accounts to prevent unauthorized disclosure through negligence.

Retention and Disposal

Retention policy of personal data shall be implemented for every personal data collected and processed by the university. Retention policy shall be defined based on the type of personal data being stored as well as its purpose. Retention policy should be consistent for similar types of personal data and processing purpose regardless of the location and unit storing and processing the data. Such policy shall also be consistent and compliant with all legal requirements under the law as well as all advisory opinions issued by the National Privacy Commission with respect to retention of personal data. The Data privacy office shall be given a monthly report of all purging of personal data by each unit duly certified by their unit heads in terms of the integrity of the report. This shall serve as a record of compliance to the Data Privacy Act. Proper disposal shall be exercised by each unit when disposing of personal data. Disposal of paper based documents shall be in the form of industrial level shredding while disposal of electronic records shall keep in mind the need to perform data scrubbing on the storage media, disposal of records in backup medium, as well as determining if such records are potentially left in online storage solutions such as cloud drives as well as email accounts (inbox, sent items, trash) and online forms.

With regards to the perpetual retention of student records by the university registrar, the university is citing **National Privacy Commission Advisory Opinion 2017-24**, specifically the following statement in the opinion:

> Retention of personal data shall only for as long as necessary:
>
> (a) for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
>
> (b) for the establishment, exercise or defense of legal claims; or
>
> (c) **for legitimate business purposes, which must be consistent with standards followed by the applicable industry** or approved by appropriate government agency.

It is the opinion of the university that the retention of student records in perpetuity is a legitimate business purpose and is consistent with the standards followed by the academic community.

No personal data shall be retained or stored in personal storage locations of the employees of the university unless otherwise granted exemption by the Chancellors Council of the university. Personal storage locations can include the following:

- Personal email accounts
- Personal cloud drive accounts

- Personal laptops or mobile devices
- Personal USB media storage devices

Documents containing personal data shall not be brought out of the premises of the university unless otherwise granted exemption by the Chancellors Council of the university.

Data Retention of Student Data

All student data are transferred to the Office of the University Registrar upon acceptance and enrollment. Such data is stored by the university in perpetuity as needed by general practices of registrars of universities. Although there is a clause on not allowing perpetual storage of personal data under RA10173 for undeclared and unforeseen purposes, the university is applying the National Privacy Commission Advisory Opinion 2017-24 as a basis for the storage of the personal data in perpetuity which includes the Diploma and the Transcript of Records of the student.

Data Retention of Faculty Data

All applicant/employee data are maintained by the Office of Vice Chancellor for Academics upon acceptance. Such data is stored by the university in perpetuity as to provide a service to support requirements of the data subject for their right to access, right to correct, right to data portability as in the case of benefits claims document requirements of the data subject. Although there is a clause on not allowing perpetual storage of personal data under RA10173 for undeclared and unforeseen purposes, the university is acquiring the consent of the data subject as the purpose is clearly declared and foreseen as previously stated.

All applicants that were not accepted, the personal data collected of the applicant shall be kept for a period of 1 year from application period so as to allow for pooling of applicants to reapply at a later time if they decided to do so. Upon the lapse of the 1 year period, paper documents shall be shredded for secure disposal. Electronic records shall be deleted securely as well.

Data Retention of CAP Data

All applicant/employee data are maintained by the Office of Personnel Management upon acceptance. Such data is stored by the university in perpetuity as to provide a service to support requirements of the data subject for their right to access, right to correct, right to data portability as in the case of benefits claims document requirements of the data subject. Although there is a clause on not allowing perpetual storage of personal data under RA10173 for undeclared and unforeseen purposes, the university is acquiring the consent of the data subject as the purpose is clearly declared and foreseen as previously stated.

All applicants that were not accepted, the personal data collected of the applicant shall be kept for a period of 1 year from application period so as to allow for pooling of applicants to reapply at a later time if they

decided to do so. Upon the lapse of the 1 year period, paper documents shall be shredded for secure disposal. Electronic records shall be deleted securely as well.

Data retention of Legal Guardian Data

All personal data collected of the legal guardian of enrolled students shall be retained for course of the duration of the university life of the student. Once the student graduates, such personal data shall be disposed of in a secure manner.

Data Retention for Visitor Data

The CCTV recording is kept for a maximum of 60 days while the logbook and online visitor management system data are kept for a maximum of 3 years after the point of data collection. Disposal of your personal data are done in a secure manner where the logbooks are shredded and digital data wiped securely. For website visitors please refer to our privacy policy as published in our website.(http://www.dlsu.edu.ph/legalities/privacy.asp)

Blocking and Erasure of Personal Data

The data subject can exercise their right to blocking or erasing of personal data collected and maintained by the university. In exercising such right, the data subject shall first raise their concern to the unit involved to request for blocking or erasing of the personal data stored. The Data privacy office shall be given a monthly report of all blocking or erasing requests by each unit duly certified by their unit heads in terms of the integrity of the report. This shall serve as a record of compliance to the Data Privacy Act. In the event that there is ambiguity in the process of correcting personal data, the data subject may directly contact the Data Privacy Office with regards to their concern for proper routing of request. In cases when the request to block or erase personal data contradicts previously collected consent or defined legitimate purpose and proportionality, no actions shall be taken until the request has been reviewed and approved by higher management.

Portability of Personal Information

Copy of Personal Data that is duly collected and stored by the university can be given to the data subject upon request (after validation of identity and availability of personal data). The format that is to be used for portability shall only consider human readability but not necessarily application readability for cases such as data migration or integration.

Acquisition of products and services from Third-parties (Supplier Relationships)

In contracting services to third party providers, stipulations on data sharing and the data lifecycle should be incorporated into the contract. Stipulations shall include the following:

1. How personal data is being collected
2. How personal data is being used or processed

3. How personal data is being stored
4. Is the personal data being shared or disclosed to fourth parties
5. How long should the personal data be retained
6. How will the personal data be disposed of after its retention period

For cases when the third party clearly stipulates that personal data may be stored in locations where data privacy laws are not yet legislated, the university should define its compensating measures if it chooses to continue with the said third party contractor.

Systems Acquisition, Development, and Maintenance

In acquiring or developing systems for the university, the system should be evaluated based on the following key components to ensure proper security profile for the system to preserve its confidentiality, integrity, and availability. (based on Microsoft and ISC^2 security profile).

- Input Validation mechanism
- Authentication mechanism
- Authorization mechanism
- Defense In Depth mechanism
- Separation of duties by design
- Configuration Management mechanism
- Session Management mechanism
- Cryptography mechanism
- Exception Management mechanism
- Failing Secure mechanism
- Auditing and Logging mechanism
- Openness of the design
- Identification of the weakest link
- Identification of single point of failure

Research and Data Privacy

In pursuing research, the following guidance should be considered by the research team.

1. As stated in section 5.3c of the IRR, RA10173 shall not apply to **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, and only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned.
2. As stated in section 20.c of the IRR, personal 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.

3. As stated in section 37 of the IRR, the fundamental privacy rights of the data subject 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.

Anonymization and Analytics in Research

In accordance with NPC Advisory Opinion No. 2017-027 (https://privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-027.pdf), the following serves as guidelines on when anonymization efforts are considered sufficient.

1. Information is anonymous when such information "does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable." Both Regulation (EU) 2016/679, which repeals the 1995 EU Directive upon which the DPA is based on, recognizes that "the principles of data protection should not apply to anonymous information."
2. The data must be stripped of sufficient elements such that the data subject can no longer be identified. More precisely, the data must be processed in such a way that it can no longer be used to identify a natural person by using "all the means likely reasonably to be used" by either the controller or a third party. An important factor is that the processing must be irreversible. The focus is on the outcome: that data should be such as not to allow the data subject to be identified via "all" "likely" and "reasonable" means. Reference is made to codes of conduct as a tool to set out possible anonymization mechanisms as well as retention in a form in which identification of the data subject is "no longer possible.
3. It should prevent all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset. Generally speaking, therefore, removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible. It will often be necessary to take additional measures to prevent identification, once again depending on the context and purposes of the processing for which the anonymized data are intended.
4. It must be clear that 'identification' not only means the possibility of retrieving a person's name and/or address, but also includes potential identifiability by singling out, linkability and inference. Furthermore, for data protection law to apply, it does not matter what the intentions are of the data controller or recipient. As long as the data are identifiable, data protection rules apply.
5. If the university collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties.

But if the data controller would delete the raw data, and only provide aggregate statistics to third parties on a high level, such as 'on Mondays on trajectory X there are 160% more passengers than on Tuesdays', that would qualify as anonymous data.

6. Anonymized data, in its truest sense, is not considered as personal information and thus, falls outside of the ambit of the DPA. However, for the proposed collection of data on demographics (age, sex, gender, and location) for marketing analytics, there is a need to further analyze and determine if this dataset is genuinely anonymized data as the original raw data containing identifiers for this dataset may still exist.
7. The manner by which such data will be collected, and whether in the process, the university will have access to the database containing complete records, including personal data that has not yet been anonymized should be considered. If the university has access to the complete records, then the fact that the processing results in anonymized data, would not exempt the university from the coverage of the data privacy act.

Inquiry and Complaints

As the data subject interact with the university, changes in the privacy manual or differences in privacy practices will be made aware thru privacy notices and other related avenues of dissemination. If the data subject are unsure about the practice, it is important that you as the data processor or the data subject seek clarification thru the Data Protection Officer. All inquiry and complaints with regards to collection, processing, storage, disclosure, and disposal of personal data shall be coursed to the Data Privacy Office for proper handling.

DPO Contact Details
Office Number: (632)4658908
Local Number: (632) 524-4611/4658900 Local 811
Email: privacy.officer@dlsu.edu.ph

Privacy Management Program

General Overview

Introduction

For the purposes of safeguarding the fundamental privacy rights of our data subjects as well as in compliance with the Data Privacy Act of 2012 within De La Salle University Manila, the boundaries of the Privacy Management Program are defined as follows: De La Salle University Manila is an academic university that provides education for primary up to graduate levels. De La Salle University also undertakes research activities that aims to serve the public interest of the nation. All activities of De La Salle University Manila such as teaching, research, administrative activities, and partner interfacing services will be covered by the privacy management program covering the Manila, Makati, Bonifacio Global City, and Laguna campuses.

Objective

The objective of managing data privacy is to ensure compliance with regulations and minimize business damage by preventing and minimizing the impact of privacy incidents. In deploying the De La Salle University Privacy Management Program, the university administration aims to develop visibility of existing privacy risks and exposures and to maintain or reduce existing risks to an acceptable level and ensure that new and changing risks or exposures are managed in an equally consistent and professional manner.

Purpose

The purpose of the program is to protect both De La Salle University and its data subjects from risks to data privacy, whether from internal or external sources, deliberate or accidental. Protection of personal data privacy is set out in terms of:

- Confidentiality: ensuring only persons who are authorized have access to the personal data are given access.
- Integrity: ensuring the purity, accuracy and completeness of the personal data collected, processed, and stored.
- Availability: ensuring personal data, associated assets, and systems can be accessed when required by authorized persons as well as the request of the data subject.
- Regulatory: ensure compliance with regulations, laws and codes of practice in the country that De La Salle University operates in as well as regulations, laws and codes of the origin countries where the data subjects of the university are from. In particular De La Salle University shall:
    - Ensure that De La Salle University management and employees comply with the requirements of the privacy manual.
    - Minimize the risk of damage to university assets, information, reputation, hardware, software or data.

- Set out clearly the university's policies relating to all aspects of the management of personal data in information and communication systems as well as those in paper form.
- Define a systematic approach to privacy impact assessment by identifying a method that is suitable to the privacy management program, the identified university data privacy, legal and regulatory requirements.
- Setting policy and objectives for the privacy management program to reduce risks to acceptable levels. Determining criteria for accepting the risks and identifying the acceptable levels of risk. The Data Protection Officer has direct responsibility for maintaining the Privacy Policy and providing advice and guidance on its implementation. All unit heads are directly responsible for implementing the Privacy Policy within their departments or unit areas, and for adherence by their staff. It is the responsibility of each member of staff to adhere to the Privacy Policy. The overall responsibility for ensuring that the Privacy Policy is implemented, developed and reviewed effectively rests with the University Chancellor. This responsibility will be delegated throughout the administrative structure reflecting the continued commitment to preserve and protect the privacy rights of the data subjects at all levels throughout De La Salle University.

Scope

Privacy management program shall include but not be limited to the following areas:

1. Privacy management program budgeting and staffing;
2. Organizational Structure for Data Protection
3. Data Classification and Governance
4. Consent Management
5. Contract Management
6. Privacy Risk and Impact Assessment
7. Retention Period and Disposal Monitoring and Enforcement
8. Internal Privacy Compliance Audit
9. Breach Management Drills and Reviews
10. Privacy Manual Review

Roles and Responsibilities

De La Salle University shall implement and maintain a comprehensive privacy management program that includes privacy management processes and procedures. The university shall establish and maintain a framework to ensure that data protection strategies within the university are aligned with its mission and objectives and comply with the applicable laws and regulations. De La Salle University shall ensure that all members of the workforce are trained in privacy and data protection matters. The various offices of the university shall develop the specific data protection procedures to address their specific circumstances, as required and to be approved by the administration of the university.

Privacy Management Program Budgeting and Staffing

De La Salle University's management shall provide assistance to its departments and offices in ensuring adequate budget and staffing levels for data protection and privacy compliance. The Data Protection Officer shall regularly review budgets and staffing levels and make recommendations as needed for approval of the administration.

Data Protection Council

A data protection council shall be formed thru a composition of one representative from each of the various existing councils of the university and convened on a quarterly basis in order to discuss issues, concerns, and suggestions on the implementation of data protection mechanisms and compliance activities.

Data Privacy Governance

De La Salle University shall:

- Provide data protection policies, standards and implementation guidelines to support data privacy governance;
- Review all data protection policies, standards and implementation guidelines prior to implementation and create a privacy exception process for the university departments and offices;
- Develop and maintain a privacy management program that adequately supports the mission and objectives of the university;
- Develop and maintain data protection strategies in support of the overall university mission statement that address changes to technology, business requirements, and laws and regulations;
- Obtain the university's senior management commitment and support for data protection and data privacy throughout the organization;
- Ensure that definitions of data protection roles and responsibilities throughout the university include privacy management program activities;
- Establish reporting and communication channels that support data protection and privacy management program governance activities;
- Audit all critical university applications and systems on a regular basis.

Document Review Requirements

Documents generated by the university such as but not limited to application forms, survey forms, brochures, publications, online or social media postings, contracts, or announcements that contain personal data shall be subject to the review of the Data Privacy Office in order to ensure compliance with regulatory requirements.

Consent Management

The university shall develop and implement consent management considering the lifecycle of a consent. Consent by definition should be freely given, specific, and recorded for it to be valid.

Collection

Collection of consent shall be performed in the following manner:

1. Student consent shall be collected during admissions application. Every attempt to gather consent shall be taken thus collection can be done during submission of application forms, taking of entrance exams, confirmation of application and admission, and upon enrollment of the student into the university.
2. Consent for employees shall be collected upon the on-boarding process of the university.
3. Student consent shall be collected from their legal guardian if they are of minority age and directly from the student upon their transition to the age of majority (18 years old).
4. Collected consent shall be recorded in either paper or electronic form and proper security measures shall be put in place to ensure its confidentiality, integrity, and availability.
5. An electronic copy of the consent shall be maintained by the Data Privacy Office as part of its consent management program.
6. Additional consent shall be collected per activity or event when there is a separate collection of personal data or when the purpose of use of the personal data significantly differs from the originally collected consent.

Implementation

In implementing the consent collected from the data subject, the university shall ensure compliance within thru regular orientation and awareness campaigns with regards to the extent of collected consent. For third party partners, consent shall align with their respective contracts or data sharing agreements to ensure that the consent can be fully implemented and enforced with the partner.

Revocation

It is within the right of the data subject to revoke their given consent at any given time with the following limitation:

1. Revocation is 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.
2. Revocation is not applicable when the personal data is needed in compliance with other relevant laws and regulations with which the university is subject to.

To exercise the revocation of consent, the data subject shall inform the Data Privacy Office providing the following details:

1. Name of data subject
2. Reason or Rationale for revoking consent
3. Effectivity date of the revocation
4. Department or Unit or Process with which the consent is to be revoked.

Revoking consent shall take effect within a period of 7 days and the Data Privacy Office shall inform the affected unit or department within the given time that consent has been revoked. The data subject shall also be informed of the needed time for the revocation to take effect.

Personal Data Inventory

Each department or unit in the university shall maintain its personal data inventory as required by RA10173. The personal data inventory is used to provide visibility of personal data that is being collected and processed by the university. It will also provide the data flow of the personal data that will allow for proportional implementation of security controls. The personal data inventory shall contain the following attributes:

- Data Element or Form Field being collected and processed.
- Classification of the data element shall be based on the data classification stated in this manual.
- Source where the data element is collected from.
- Purpose of collecting and processing of the data element.
- Legal Basis for the collection and processing of the data element.
- Location where the data element is being stored.
- List of internal users who process the data element.
- List of PIPs that are given access to the data element.
- List of other PICs that are given access to the data element.
- Policy the governs the use and disclosure of the data element.
- Protection mechanisms or controls currently existing for the data element.
- Backup mechanisms for the data element.
- Retention period for the data element.

The personal data inventory shall be reviewed on an annual basis to maintain is accuracy with respect to actual operations.

Privacy Risk and Impact Management

Risk is a function of threats exploiting vulnerabilities to obtain, damage or destroy assets. Thus, threats (actual, conceptual, or inherent) may exist, but if there are no vulnerabilities then there is little/no risk. Similarly, one can have a vulnerability, but if there is no threat, then one has little/no risk.

Risk is calculated as the likelihood multiplied the impact for a specific threat exploiting a vulnerability, where likelihood can further be divided into likelihood of attack from a threat and likelihood of success of an

attack (based on threats and vulnerabilities). Where Impact can be divided on impact on Confidentiality, Integrity, and Availability

De La Salle University shall develop a privacy risk and impact management plan and program. Specifically, the university's departments and offices shall:

- Implement a systematic, analytical and continuous privacy risk and impact management program for information included in the scope of the Data Privacy Act of 2012;
- Ensure that risk identification, analysis and mitigation activities are performed;
- Ensure that risk and impact assessments are performed periodically to evaluate effectiveness of existing controls as well as the accuracy of existing exposures;
- Define strategies and mitigate impact and risks to acceptable levels for the university; and
- Report significant changes in risk and impact levels including significant changes in threats and vulnerabilities on both a periodic and an event-driven basis.

The risks that needs to be considered are as follow based on the punishable acts of RA10173:

- Unauthorized Disclosure
- Unauthorized Purposes
- Unauthorized Processing
- Access due to Negligence
- Malicious Disclosure
- Improper Disposal
- Intentional Breach
- Concealment of Breach
- Incorrect information stored
- Loss of Information due to intentional and non-intentional acts.

The list of threats that needs to be considered are as follows (but not limited to):

- Malicious and Non-malicious internal personnel or student
  - Shoulder surfing
  - Part of talking points with friends and family
- Acts of God or Nature
- Internal and External Hacking
  - Phishing
  - Negligence and malware infection
- Theft by individuals within and outside of the campus
- Third Party Provider misuse of data
- Please classify whether its Confidentiality, Integrity, Availability

The list of vulnerabilities that needs to be considered are as follows (but not limited to):

- Unknown or unclassified information
- Lack of existing policies and procedures
- Inconsistent implementation of policies and procedures
- Lack of awareness training / campaign
- Lack of physical or technical controls
- Lack of time and/or resource to implement policies and procedures
- Urgent needs and demands that contradict compliance
- Negligence of individuals
- Limitation of capabilities of processes and resources (really not possible)
- Lack of Data Sharing Agreement or Internal Sharing Policy

In determining Impact, the following definitions will be used (based on ISO 29134:2017 and NPC Privacy Toolkit)

1. Negligible – The data subjects will either not be affected or may encounter a few inconveniences which they will overcome without any problem.
2. Limited – The data subject may encounter significant inconvenience which they will be able to overcome despite a few difficulties.
3. Significant – The data subjects may encounter significant inconveniences which they should be able to overcome but with serious difficulties.
4. Maximum – The data subjects may encounter significant inconvenience or even irreversible consequences which they may not overcome.

In determining likelihood or probability, the following definitions will be used (based on ISO 29134:2017 and NPC Privacy Toolkit)

1. Unlikely – Not expected, but there is a slight possibility it may occur at some time.
2. Possible – Casual occurrence. It might happen at some time.
3. Likely – Frequent occurrence. There is a strong possibility that it might occur.
4. Almost certain – Very likely. It is expected to occur in most circumstances.

After the risk has been computed, the resulting assessment should be plotted in the following matrix to determine prioritization of remediating actions. All risks that are in the "RED" quadrant should be prioritized for corrective and preventive actions or controls. All risks that are in the "GREEN" quadrant are candidates for maintenance of status quo. All risks that are in the "YELLOW" quadrants shall be further evaluated to determine if further actions need to be taken to reduce the risks. This is based on a balanced risk appetite and tolerance.

	Unlikely	Possible	Likely	Almost Certain
Maximum				
Significant				
Limited				
Negligible				

The privacy impact assessment shall be reviewed on an annual basis or when there is a new project or significant change in order to maintain its accuracy with respect to operations.

Personal Data Processing Systems Registration

Personal Data Processing Systems can be in paper, simple spreadsheets, or information systems that the university uses. Any system that contains at least 1,000 sensitive personal information shall be registered with the Data Privacy Office as such systems would need to be provided proper and proportional security controls.

Sharing or Disclosure of Personal Data

Sharing of personal data or documents containing personal data shall be kept to a minimum as needed and guided by the existing policies, consent statements, and contracts that have been put in place. Any request for personal data that does not conform to existing legal basis for sharing shall not be entertained unless approval or exception has been requested and approved by the Data Privacy Office.

Retention Period and Disposal Monitoring and Enforcement

Each unit in the university shall maintain and implement a retention policy for the personal data that is being collected and processed by each respective unit. The retention policy and its period shall be clearly communicated to all employees or members of the unit to ensure awareness and compliance with the units own retention policy. Disposal of personal data shall be validated by the Data Privacy Office and a certificate of disposal shall be generated duly signed by the Data Protection Officer. Periodic physical audits shall be conducted to ensure compliance and personal data is not retained beyond the stated retention period. Improper disposal may lead to punishable acts under RA10173.

Internal Privacy Compliance Audit

The university develops, disseminates, reviews & updates:

- A formal, documented audit and accountability policy;
- Processes to facilitate the implementation of the audit and accountability policy, procedures and associated controls;
- Name a person or role as the responsible party for the overall audit process and its results;
- Determine the appropriate scope of audit controls that are necessary to protect organizational resources and ensure compliance requirements are met;
- Determine what data will need to be captured by the audit controls and logs; and
- Implement hardware, software, and procedural controls that record and examine activity.

Internal audit shall be conducted at least on an annual basis.

Breach Management Drills and Review

De La Salle University shall develop and maintain an incident and breach management plan and program for detecting, identifying, analyzing, and reporting privacy and information security related events. Drills shall be conducted at least once a year as part of compliance to NPC requirements. Further specifications are detailed in the university's Incident and Breach Management plan. The university shall:

- Establish, maintain and implement procedures for documenting incidents and breaches as a basis for subsequent investigation and in compliance with the Data Privacy Act; and
- Manage post-incident and breach reviews ("lessons learned") and document incident and breach causes and recommended corrective and preventive actions, in consultation with the Data Protection Officer.

Privacy Manual Review

The privacy manual shall be reviewed on an annual basis by the Data Privacy Office in consultation with the community in order to ensure its relevance and accuracy in compliance with regulatory requirements as well as organization mandates. Upon revision, the history of the changes should be tracked and the updated privacy manual shall be recommended for approval by the appropriate council in the university.

Breach Management Plan

This document serves as the definitive guide to the privacy incident response and management plan for De La Salle University Manila to include external campus in Makati, BGC, and Laguna. This privacy incident response plan describes the actions that administrators, faculty, students, staff, as well as third party Personal Information Processors (PIP) are to follow for an incident that could represent, but is not limited to, unauthorized personal data access and/or use of such systems in violation of the university privacy policy and acceptable use policy. A privacy incident may originate from, be directed towards, or transit university boundaries and resources.

Types of Privacy Incidents

Signs of a privacy incident may be obvious or subtle. Privacy incidents can both be electronic or non-electronic in nature. Some privacy incidents are not immediately visible or noticeable but can present itself over time and indirectly compromise the privacy of personal data. Thus, any unusual activity, irregularity, or unplanned/unapproved change to policies, procedures, forms, and configuration of systems or applications can signify an incident that can potentially lead to a breach.

Privacy incidents can include, but are not limited to, any of the following events:

- Unauthorized collection of personal data
- Negligence in processing and/or disclosure of personal data
- Unauthorized, unaccompanied person(s) present in the work area, Personal Data Store Room, or Data Center
- Unauthorized access to personal data processing facility and systems.
- Observance of negligence such as leaving filing cabinets with personal data unattended and unlocked, or leaving documents containing personal data on the table that can be easily seen by other people.
- Observance or detection of unusual or suspicious network or system activity by ITS.
- Unauthorized access to or possession of personal data
- Improper or Unauthorized sharing of personal data thru non-technological means such as casual conversations or technological means such as email, messaging services, or cloud storages.
- Improper release of personal data or related information that can be used to obtain it such as sharing outside of limits of stated policies like the use of personal accounts or use of unsecured communications channels (e.g. misdirected emails, Unsecure emails, misdirected fax or print jobs, unauthorized disclosures, loss of storage devices).
- Improper disposal of personal data such as reuse of paper documents with personal data as gift wraps or scratch papers or improper disposal of storage devices containing personal data.

- Violation of defined retention periods for the storage of personal data
- Lapses in safekeeping of personal data while within retention period.
- Disaster (ex. hazardous materials, fire, flood, tornado, hurricane, or other disaster) that either places staff or confidential information at risk or prevents normal security procedures from taking place.

Types of Breaches

A privacy incident is escalated into a privacy breach (that may lead to notification of the NPC) when the following conditions are met:

1. Personal Data is involved in the incident
2. Such personal data is known to have been accessed by an unauthorized person or group of persons or entity.
3. Access to such personal data can lead to serious harm to the data subject.

As defined by the DPA, the following are breaches that are punishable by law:

1. Unauthorized Processing of Personal Information and Sensitive Personal Information.
2. Accessing Personal Information and Sensitive Personal Information Due to Negligence.
3. Improper Disposal of Personal Information and Sensitive Personal Information.
4. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes
5. Unauthorized Access or Intentional Breach
6. Concealment of Security Breaches Involving Sensitive Personal Information
7. Malicious Disclosure
8. Unauthorized Disclosure
9. Combination or Series of Acts

Incident Management Team Members Roles and Responsibilities

All Members of the Community (Administrators, Faculty, Staff, Students, PIPs)

- Watch for signs of privacy incidents and report any irregularities or suspicious activity immediately to the supervisor according to the instructions in this document.
- Raise questions on any unclear situations that involve the handling of personal data to the supervisor.
- Review this document at least on a bi-annual basis to keep up to date with updates and changes to the plan.
- Detection can be done thru:
    - Direct observation
        - Unauthorized, unaccompanied person(s) in the work area Personal Data Store Room, or Data Center

- Unauthorized access to personal data processing facility and systems (e.g. lack of consent)
- Observance of negligence such as leaving filing cabinets with personal data unattended and unlocked, or leaving documents containing personal data on the table that can be easily seen by other people.
- Improper or Unauthorized sharing of personal data thru non-technological means such as casual conversations or technological means such as email, messaging services, or cloud storages.
- Improper release of personal data or related information that can be used to obtain it such as sharing outside of limits of stated policies such as use of personal accounts or use of unsecure communications channels (e.g. misdirected emails, Unsecure emails, misdirected fax or print jobs, unauthorized disclosures, loss of storage devices).
- Improper disposal of personal data such as reuse of paper documents with personal data as gift wraps or scratch papers or improper disposal of storage devices containing personal data.
- Personal Data processing systems not functioning properly
- Lack of awareness of personnel handling personal data

o Third-Party Reports
- Unusual activity or characteristic or output of personal data processing systems
- Unavailability of personal data processing systems
- Incorrect personal data stored
- Complaints reported due to change in policies and processes
- Potential breach as reported by data subject

Reporting Member (Administrators, Faculty, Staff, Students, PIPs)

- Promptly notify the supervisor of the incident as soon as the incident is detected.
- Remember to document the details of the incident as soon as it is reasonable to do so, and include as much detail as possible. Document all individual actions with the dates and times.
- If the reporting member suspect an incident on your computer, refrain from quitting applications or shutting down. Instead, log off and immediately report this to the supervisor.
- Refrain from trying to investigate the incident.
- Refrain from discussing the incident with others except as noted in this policy/procedure.

Supervisor / Administrator / Unit Heads

- The supervisor or administrator shall routinely or periodically perform checks on the people under their jurisdiction to determine if personal data is being mishandled either intentionally or unintentionally. Any findings should be documented and reported.

- Assess the nature and extent of the incident and determine if the compromise involves personal data.
- Perform initial containment of the incident and determine if it constitute as a breach.
- In the event of a breach, escalate the incident immediately to the Data Protection Officer.

Breach Team

- The breach team shall be composed of the Data Protection Officer, the Chancellor, the University Legal Counsel, the ITS Director if it involves university systems, and the involved unit heads and their corresponding superiors.
- Contain the breach and assess the extent and the amount of exposure or damages that could potentially be incurred due to the breach.
- Determine if there is a need to notify the data subject of the breach and act accordingly.
- Determine if there is a need to notify the National Privacy Commission of the breach and act accordingly.
- Determine if there are other regulatory bodies that needs to be notified of the breach (e.g. foreign consulate if it involves a foreign citizen, CHED)
- Ensure all evidences are properly collected and chain of custody is documented.
- Determine corrective and preventive actions.
- Document all activities that occurred as part of the breach report.

Identification and Assessment

When conducting the initial assessment of the incident, the following are recommended guidelines to be performed by the Supervisors, Administrators, Unit Heads:

1. Determine if personal data is involved. Please refer to the definitions on personal information and sensitive personal information.
2. Determine source and nature of incident or breach.
3. Determine if the incident resulted in a breach:
    a. If it is a breach:
        i. Determine the number of personal data that may have been compromised. Provide basis for assertion on number of compromised personal data. Provide also details of types of personal data involved in the incident (e.g. actual fields or columns of a spreadsheet)
        ii. Classify compromised data accordingly (Personal Information, Sensitive Personal Information).
        iii. Determine if there are any security controls in place on the compromised personal that may limit or prevent its misuse.
        iv. Determine if the personal data can potentially be used by unauthorized personnel (e.g. Flash drive containing

personal data has been lost or stolen, online DLSU account has been hacked)
v. Ensure breach data collection adheres to a chain of custody for evidence purposes.

b. If it did not result into a breach:
i. Collect data on the event for documentary and review purposes

4. Ensure proper documentation of incident or breach.

Containment Strategies

After determining the extent of the incident or breach, the following containment guidelines can be performed by the Supervisors, Administrators, Unit Heads:

1. If the incident did not result into a breach
   a. Immediately perform corrective actions and document/log the incident and corrective action performed. Corrective actions can include the immediate shredding of personal data beyond retention period, or removing unauthorised personnel from personal data store room, or immediate cessation of negligent activity.
   b. If the incident relates to technical issues such as the spread of a malware or ransomware, immediate notification to the ITS should be performed.
   c. If the incident involves disclosure due to negligence, immediate discontinuation of activity should be performed and notification should be given to the DPO.
2. If the incident resulted into a breach
   a. If it is a technical breach, immediately consult with ITS and DPO for corrective actions.
   b. If it is a policy or procedural breach, immediately consult DPO.
   c. Convene the Breach Management Team to determine the next course of action that may include notification of the data subjects as well as NPC.

Escalation Procedures

The incident escalation procedure follows the hierarchical structure of the organization. All observed discrepancies from compliance requirements are immediately reported to their direct supervisors for initial assessment and containment with the exception of technical issues where they are directly reported to the ITS as well. In case the initial assessment determines that the incident resulted into a breach, the DPO shall be notified immediately and if it involves technical concerns, the ITS Director shall be notified immediately as well. The DPO shall determine the immediate course of action to contain and further validate the breach and shall consult the Breach Team (consisting of the Chancellor, Legal Counsel, ITS Director) for further necessary actions such as notification to data subject and NPC. If determined necessary, notification to NPC shall not exceed 72 hours from the recorded time of the breach notification.

Preservation of Evidence

In the event of a breach, the following information should be gathered and preserved in order to aid in investigation, containment, remediation, recovery, and review.

1. Information about the discovery of the breach to include:
    - Name of person who discovered the breach
    - Name of person who validated the breach
    - Source of breach
    - Method and Type of Breach
    - Date and Time of discovery
    - Name of person who escalated to DPO
    - Date and Time of escalation to DPO
2. Collection of document or technical evidences that may include but not limited to the following:
    - Any logs of phone calls, emails, messaging that can show or cause the compromise
    - Any copy of actual malware involved
    - IP addresses of devices involved thru logs
    - CCTV footages
    - Photographs taken
    - Failed storage units
    - Initial containment actions taken
    - Data Subjects involved in the breach
3. When handling any of the information previously stated, it is important that the logs be handled by the unit head and to be validated by the DPO to ensure proper chain of custody. It is important to log every exchange or transfer of information related to the breach in order to preserve the validity of the information.
4. The final copy of evidences shall be kept by the DPO.

Incident / Breach Recovery and Remediation Process

The remediation and recovery phase of the breach assumes that initial containment and notification processes have been performed. In the recovery phase it is important to distinguish recovery by the type of breach:

Confidentiality

In the event that the breach is the loss of confidentiality of personal data. It is important to determine how the loss can affect the data subject. It should be considered that modification of certain information be performed in order to reduce potential risks of loss of confidentiality. If this is not possible or is insufficient to remediate and recover from the breach thru modification alone, then other actions should be considered including notification of relevant departments and agencies of the breach aside from the data subject and NPC to reduce the possiblity of misuse of the personal data (e.g. identity theft) Recovery can also consider retraction of data sent to third parties if unauthorized as well as implementation of privacy agreements to compensate.

Integrity

When data integrity is compromised, it is important to look at the chain of events and affected data subjects as well as systems and processes. Requests for correction to the stored personal data shall course thru the DPO to facilitate its proper updating. In cases when loss of integrity results in the unavailability of correct data, the recovery process shall be reclassified under availability.

Availability

Loss of availability can either be the loss of the service providing the personal data or the loss of the personal data itself. Restoration process from backups shall be initiated. In order to reduce the possiblity of encountering unrecoverable data, it is recommended that testing be done regularly on the backups. If the source of personal data is on paper, it is recommended that digitization be considered as a backup and restoration mechanism.

Incident / Breach Prevention

To prevent breaches from occurring, the following are recommended steps to take:

1. Conduct regular awareness campaigns
2. Create a Personal Data Inventory to allow a clear understanding and awareness on data collected and processed
3. Create a Privacy Impact Assessment in order to aid in prioritization of controls based on risk levels
4. Assess availability of policies, processes, and procedures that will govern the collection and processing of personal data. Develop such policies, processes, and procedures as needed with the approval of the Data Privacy Office.
5. Create a RACI (Responsible, Accountable, Consulted, Informed) matrix so as to have clarity on the responsibilities of each individual in collecting and processing personal data.
6. Create a data classification scheme in order to be clear on how to handle data.
7. Employ technical controls such as encryption as determined thru the PIA to reduce risks and impact of breach
8. Make the reduction or limiting of collection of personal data as the first course of action rather than the use of consent statements
9. Limit access to personal data
10. Limit processing performed on personal data
11. Keep details records or logs of the activities that deals with personal data.
12. Perform continuous assessment on PDI, PIA, Data Life Cycle, as well as security controls in place.

Post Incident / Breach Review

After every incident or breach, it is important that a review process be conducted in order to allow for continuous improvements to be done as well as put in place preventive actions that can reduce the possibility of the

incident or breach occurring again. When conducting the review, it is important to refer to the incident / breach report as well as the evidences and its chain of custody to determine the root cause of the incident or breach. The review should be conducted within 72 hours of the reported incident or breach in order to comply with the notification / reporting requirements of NPC.

Incident / Breach Response Plan Test

To ensure appropriateness and awareness of the breach management plan, drills or tests shall be conducted initially on a semi-annual basis to aid in the awareness and refinement of the plan. Upon stabilization, the test can be done annually.

Incident / Breach Response Plan Review

The breach management plan is currently in its initial stages of development. As such, it is important that the review of the plan be carried out on a quarterly basis to ensure the appropriateness of the plan. Upon stabilization of the plan, it is recommended that the review be conducted on an annual basis in order for the plan to consider environmental and business changes that may affect the plan or whenever a significant change in processes and policies occur.

Emergency Cases Note

- Protection of Vital Interests
  - Access to personal information is allowed to protect vital interests of the data subject including his her life or health
  - Access to sensitive personal information is allowed to protect the life and health of the data subject or another person and the data subject is unable to express consent
- Public Order and Safety
  - Access to personal information is allowed to respond to national emergency or to comply with the requirements of public order and safety as prescribed by the law
  - Access to sensitive personal information is NOT ALLOWED by default and consent should be collected prior to processing.
- Medical Treatment
  - Access to personal information and sensitive personal information is allowed for processing for necessary medical treatment provided that the processing is provided by a medical practitioner or institution and an adequate protection of personal data is ensured.
- Public Authority
  - Access to personal information is allowed for fulfillment of constitutional or statutory mandate of a public authority
  - Access to sensitive personal information is allowed for the protection of the lawful rights and interests of the persons in court proceedings or legal claims or when provided to public authority pursuant to a constitutional or statutory mandate.

- Legal Obligations
  - Access to personal information is allowed for compliance with legal obligations for which the PIC is in the interest
  - Access to sensitive personal information is allowed as provided by existing laws and regulations that do not require consent and that guarantee the protection of personal data.

Breach Penalties

See section 52 to 65 of the IRR of the Data Privacy Act of 2012.

Version History

Version	Date Updated	Changes Made	Changed By	Approved by
1.0		Initial development of the Privacy Manual	Data Protection Officer	