University of Southeastern Philippines

Knowledge Management Systems Division

Data Privacy Manual

PART 1. BACKGROUND

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect Personal information in information and communications systems both in the government and the private sector.

It ensures that entities or organizations processing Personal information establish policies, and implement measures and procedures that guarantee the safety and security of Personal information under their control or custody, thereby upholding an individual's data privacy rights.

A personal information controller (PIC) or personal information processor (PIP) is instructed to implement reasonable and appropriate measures to protect Personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

To inform its personnel of such measures, each PIC or PIP is expected to produce a Privacy Manual (Manual). The Manual serves as a guide or handbook for ensuring the compliance of an organization or entity with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the National Privacy Commission (NPC). It also encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

PART 2. INTRODUCTION

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

This Manual is hereby adopted as a testament of the University's commitment in respecting and upholding data privacy rights pursuant to the mandate of the National Privacy Commission (NPC). The Manual shall inform the clients of the University's data protection and security measures, and may serve as the clients' guide in exercising their rights under the DPA.

PART 3. DEFINITION OF TERMS

a. ***Data Subject*** refers to an individual whose personal, sensitive personal or privileged information is processed by the University/College. It may refer to officers, employees, consultants, and clients/costumers of the University/College.

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

c. ***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.

d. ***Personal Information Controller (PIC)*** refers to a personnel designated to control the collection, holding, processing, use, transfer, or disclosure of personal information.

e. ***Personal Information Processor (PIP)*** refers to any natural or juridical person qualified to act as such under the DPA and its IRR to whom the PIC may outsource the processing of Personal information pertaining to a data subject.

f. ***Data Protection Officer (DPO)*** refers to an individual tasked to monitor the compliance of the University with the Data Privacy Act, its IRR, issuances by the NPC, and other applicable laws and policies.

g. ***Privileged Information*** refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

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

i. ***Sensitive Personal Information*** refers to personal information:

i. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

ii. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

iii. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

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

j. ***The University*** refers to the University of Southeastern Philippines

PART 4. SCOPE AND LIMITATIONS

This Manual applies to the processing of personal information in which a University entity is involved. All University personnel and students must comply with all the provisions stated in this Manual. The types of personal information and the contexts of personal information processing defined in laws concerning *government transparency* and *freedom of information* shall be excluded from the coverage of this Manual.

If this Manual is found wanting of data privacy policies or provisions, the Data Privacy Act of 2012, its Implementing Rules and Regulations (IRR) and issuances by the National Privacy Commission (NPC) shall be consulted for a comprehensive set of laws and regulations applicable to a particular situation.

PART 5. GENERAL DATA PRIVACY PRINCIPLES

The University, in the course of its operations, collects the necessary Personal information of its students, alumni, employees, personnel, suppliers, contractors, consultants, among others. The Personal information collected shall be used by the University for purposes including, but not limited to, documentation, recording, and communication. The University will ensure that Personal information under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing.

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

Principles of Transparency, Legitimate Purpose and Proportionality

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

a. *Transparency* – The data subject must be aware of the nature, purpose, and extent of the processing of his/her Personal information, including the risks and safeguards involved, the identity of PIC, his/her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of Personal information should be easy to access and understand, using clear and plain language.

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

c. *Proportionality* – The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal information shall be processed only if the purpose of the processing could not reasonably be fulfilled by any other means.

PART 6. COLLECTION AND PROCESSING OF PERSONAL INFORMATION

1. Notification and Consent

As a general rule, any activity involving Personal information collection and processing must start with notifying the data subject of the nature and extent of data collection and processing. Only after satisfying this provision shall the data collection process proceed to the second essential step which is getting the data subject's consent. Generally, consent is mandatory prior to the collection and processing of Personal information, subject to some lawful exemptions. Consent given may be withdrawn. The data subject may signify consent in either explicit or implicit form:

a. Explicit consent is signified via explicit and conventional confirmation mechanisms. Common examples include consent via physical forms validated by the data subject's signature.

b. Implicit consent is acquired when it is ascertained that the data subject has been notified of the nature and extent of data collection but getting explicit consent is not possible or applicable. In such cases, it is implied that by proceeding with using a particular computer system or service, the data subject has consented with the inherent data collection that may occur.

Example: Asking consent for the use of web cookies in a website.

2. Types of personal information collected

The University collects and processes only the type and amount of personal information necessary to perform its core and auxiliary functions. As an institution composed of heterogeneous entities, the University may collect a variety of personal information in different contexts and for different specific purposes. This section lists down the common primary types of Personal information collected by the University throughout the course of its operations. In general, among the personal information the University may collect include:

a. Students' personal information
   Full name, ID number, parents' or guardians' name, home address, birthdate, email address, mobile or telephone number, nationality, signature
b. Students' academic information
   Grades, scholastic performance, courses enrolled, academic program evaluation
c. Students' medical information
   Blood type, medical history, basic laboratory test results (X-ray, drug test, etc.)
d. Employees' personal information as required in the Personal information Sheet
e. Employees' academic information
   Grades, scholastic performance, courses enrolled, academic program evaluation
f. Financial information
g. Visitors' personal information
   Full name, identification card, contact information
h. Suppliers'/contractors'/consultants' personal and business information
i. Images via Closed-Circuit Television or other similar recording devices
j. Internet Protocol (IP) addresses
k. Internet cookie session data

l. Alumni's personal information

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

3. Contexts and modes of data collection

a. University entrance application

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

b. Student admission or enrolment

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

c. Student academic evaluation

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

d. Employee application and management

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

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

e. Visitor identification

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

4. Measures for ensuring legitimacy of data collection and accuracy of collected data

All data collection activities must first be approved by the University's Data Protection Officer (DPO). After given clearance by the DPO and officially approved by the University President and/or members of the top management, the process owner of the data collection activity must take reasonable steps to ensure that all Personal information collected or processed are accurate and relevant.

Only authorized University personnel shall be allowed to perform data collection. In cases wherein data collection is initiated by an external entity not affiliated with the University, the data collection shall be done by the entity's authorized representatives subject to agreed terms and conditions.

a. Personnel Training

All personnel involved in collecting and processing Personal information must have undergone trainings and/or seminars related to the University's data privacy policies prior to performing the said tasks. The University shall ensure that a mandatory training on data privacy and security is conducted at least once a year.

b. Means for correcting or updating collected personal information

All process owners of any procedure that involve Personal information collection must follow a standard procedure for updating and correcting outdated and erroneous information to the extent allowed by all applicable laws.

c. Data entry protocol

In every undertaking involving data collection, a set of standard data entry rules must be followed to minimize the occurrence of data inaccuracy and/or breach. In the absence of a more specific data entry protocol, this general protocol must be adopted:

i. Ensure that the location or facility in which the data entry task is performed upholds the principles of data privacy. Data entry must be done away from the prying eyes of unauthorized individuals.

ii. Collection of sensitive personal information, such as medical records, must be done in a discreet manner.

iii. The personnel must review and verify the acquired data prior to officially recording and/or saving it. This applies to both manual and automated data entry.

iv. For data entry on in-house developed information systems (e.g. USePAT registration), automated mechanisms or algorithms must be incorporated to check and/or prevent syntactical, formatting, and/or data type mismatch errors.

v. Only official channels and modes of collection shall be used in recording and storing data. For instance, a normal sheet of paper shall not be used in lieu of an official data entry form and/or system, except when duly approved by the DPO.

vi. Only officially designated personnel of a particular college/office/department shall be allowed to perform data entry tasks. He/she shall not delegate such privileges to other personnel without prior approval of a supervising authority.

5. Acceptable and Lawful Use of Personal Information

Authorized University personnel are given privileges to access, use and process personal information granted that they perform such actions for legitimate purposes and within the bounds of applicable laws.

a. Due diligence

Personnel authorized to process personal information are expected to practice due diligence in all dealings involving personal information. Reasonable care shall be taken to ensure that personal information are not used to serve malicious intentions which may cause harm to the data subject and/or the University.

b. Process ownership

A process owner is an office, a department or college assigned to oversee the conduct of a procedure. To ensure that the right personnel and the right University entity are the ones performing information processing, the University shall define the official process owner of each University procedure involving personal information processing. The University's Planning, Quality Assurance, and Resource Management (PQuARM) Division shall be tasked with this duty.

i. Access rights / User privileges

The heads of offices designated as process owners shall define in an official document (e.g. Operations Manual) the list of authorized users and their level of access privileges. A user shall not be allowed to delegate his/her access privileges to another without an explicit and documented approval from the supervising authority

ii. Information systems

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

iii. Scope and interoperability of information systems

The scope of an information system must be clearly and comprehensively defined especially since the University mostly uses a centralized database system to handle the data of its information systems. A document specifying the Personal information elements of which an information system has access to shall be necessary to ensure that the information system is processing the appropriate data considering the principles of *legitimacy of purpose* and *proportionality*.

When an information system is made interoperable with another, or when a new module is integrated into an existing information system, a systems integration document shall be produced covering the implication of such activity on the scope of the system in terms of Personal information access.

Any significant addition, integration, or alteration of an information system shall be reviewed by a technical working group to be established by the KMSD.

c. Lawful processing of personal information

Personal information processing within the contexts defined in *Part 6 Section 3* of this Manual shall be deemed necessary for the University to perform its functions, serve its purpose, and pursue its legitimate interests; and shall therefore be considered lawful.

Whenever personal information processing does not fall on the said contexts, it must comply with any of the following conditions, as set by the DPA, for it to be considered lawful.

i. The data subject must have given his/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 University is subject;

iv. The processing is necessary to protect vitally important interests of the data subject, including his/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 University, or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject, which require protection under the Constitution.

d. Lawful processing of sensitive personal information

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

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 information;

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/her consent prior to the processing;

iv. The processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations provided that:

   i. Processing is confined and related to the bona fide members of these organizations or their associations;

   ii. The sensitive personal information are not transferred to third parties; and

   iii. Consent of the data subject was obtained prior to processing;

v. 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. Retention and Destruction of Personal information

Personal information shall only be retained for as long as necessary to serve its declared purpose or comply with regulatory and legal requirements. Depending on the nature of data and purpose it serves, the retention period could range from days to years.

a. Retention of student information

Students' information collected upon admission shall be retained permanently by the University in compliance with the CHED Memorandum Order No. 30, series of 2009 and in accordance with the Manual of Regulations for Private Higher Education (MORPHE) of 2008. The OUR shall be tasked to oversee the retention of student information.

b. Retention of employee personal information

Under existing Labor laws, the University is required to keep its employee records in perpetuity. The HRMD shall be tasked to oversee the retention of employee information.

c. Controls for detecting irrelevant or unnecessary Personal information

A set of detective controls which may include or be a combination of: process, human capital, physical, and/or technological controls shall be set in place to uncover irrelevant and/or unnecessary personal information, in electronic or physical format, under the custody of a particular University entity.

d. Lawful destruction of personal information

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

e. Data disposal protocol

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

i. Approval and documentation

Disposal of personal and/or sensitive data stored in physical and/or digital form contained in an official public document shall require the official approval of the data/process owner and the DPO and shall be done in coordination with the University Records Office (URO). Major data disposal activity shall be documented by the data/process owner and the office of the DPO. The documentation shall include basic details like date, justification for disposal, details of disposal, and signatures of the individuals involved.

ii. Deep (low-level) formatting of digital storage devices

Personal information contained in digital storage devices such as hard disks and flash drives shall be disposed using the latest technology and/or mechanism for deep formatting. The KMSD shall perform such disposal mechanism upon official request from a University entity. The requesting entity shall oversee the disposal procedure to ensure that no unauthorized backing up of data is performed.

iii. Decommissioning storage devices

The protocol of the University's Supply Management Unit (SMU) shall be followed in decommissioning digital storage hardware. The SMU shall ensure that decommissioned storage hardware are stored in a secure facility where only authorized personnel are given access to. All decommissioned storage devices must have undergone deep formatting from the KMSD prior to storage in the SMU storage facility. As much as lawfully possible, storage devices shall not be auctioned or sold in functional condition with disk platters intact. This is to ensure that no sophisticated recovery method can be done to recover previously stored files in the device.

iv. Shredding of paper-based documents

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

PART 7. DISCLOSURE OF PERSONAL INFORMATION

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

a. Perpetuity of confidentiality

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

b. Internal data sharing

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

c. External data sharing

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

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

d. Public disclosure of personal information

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

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

Example: Posting of personal information in social media

University employees must refrain from publicly posting personal information, especially those acquired in the performance of their duty in the University, of their co-employees and/or students in any social media platform.

PART 8. SECURITY MEASURES

The University shall implement reasonable and appropriate physical, technical, and organizational measures for the protection of Personal information. These security measures aim to maintain the availability, integrity, and confidentiality of Personal information and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

1. Organizational Security Measures

a) Designating a Data Protection Officer

Pursuant to the Data Privacy Act of 2012, the University shall designate an individual or individuals who shall function as Data Protection Officer (DPO). The DPO shall have the following responsibilities:

i. Monitor the compliance by the PIC and PIP with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies

ii. Ensure the conduct of a Privacy Impact Assessment (PIA) relative to

activities, measures, projects, programs, or systems of the PIC or PIP;

iii. Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights;

iv. Ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;

v. Inform and cultivate awareness on privacy and data protection within the University, including all relevant laws, rules and regulations and issuances of the NPC;

vi. Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;

vii. Serve as the contact person of the PIC or PIP vis-a-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;

viii. Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and

ix. Perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

b) Designating a Compliance Officer for Privacy (COP)

Each University unit shall designate a Compliance Officer for Privacy (COP) whose primary responsibility is to ensure that the personnel within his/her jurisdiction uphold the principles of data privacy and comply with the provisions of this Manual. The COP shall act as the local DPO of a particular unit as he/she is expected to perform all the functions of the DPO, as listed in the immediately preceding section, except for items (i), (ii), (iii), (vii), and (viii). The COP shall also represent his/her unit in official meetings or events concerning data privacy as may be required by the University DPO.

The COP shall serve as the DPO's local point person thus, is expected to be the primary source of notification should an incident occur in his/her jurisdiction.

c) Conducting Relevant Trainings or Seminars

The University shall conduct a mandatory training on data privacy and security at least once a year. Personnel directly involved in the processing of Personal information shall be subjected to mandatory relevant trainings as often as necessary.

d) Conducting Privacy Impact Assessments (PIA)

The University shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of Personal information. The PIA is essential to identify risks in the processing system and monitor for security breaches. The PIA plays a critical role in the implementation of the Incident Response Procedure as the mitigating measures to be performed when a particular security and/or data breach incident occurs shall be based on it. The creation of a particular PIA document shall be a collaboration between the Office of the DPO and the process owners.

Six (6) months after the effectivity of this Manual, all existing University systems and procedure that deal with personal information shall have their own official PIA documents.

e) Establishing a Data Privacy Review Team

A University Data Privacy Review (DPR) Team shall be established to regularly oversee and audit the implementation of the University's data privacy policies as defined in this Manual. The DPR Team shall be headed by the DPO, KMSD Director.

The DPR head shall initiate the selection of the other members of the DPR Team. Through a set of detective controls which may include or be a combination of: process, human capital, physical, and/or technological controls, the DPR Team shall audit the different University units to evaluate their compliance to the University's data privacy policies. The audit shall be conducted at least once a year.

f) Non-Disclosure Agreement

As part of their duty of confidentiality, all employees shall be asked to sign a Non-Disclosure Agreement (NDA). All employees with access to Personal information shall operate and hold Personal information under strict confidentiality if the same is not intended for public disclosure.

g) Review of the Privacy Manual

This Manual shall be reviewed, evaluated, and, when necessary, updated annually to be consistent with current data privacy best practices and remain compliant with the law.

2. Physical Security Measures

a) Format of Data

Personal information in the custody of the University may be in digital/electronic format and paper-based/physical format. For ease of access and as a backup mechanism, pertinent paper-based documents containing personal information shall be digitized and stored in a data server facility administered by the KMSD. The digitization shall be done by the specific University unit.

b) Storage Type and Location

All Personal information of the University's students, employees and staff, including contractual and agency-based employees, in paper-based documents shall be stored securely in a locked filing cabinet located at the particular University unit authorized to retain such documents. University units that handle a considerable amount of paper-based records, such as the OUR shall have a dedicated physical data storage facility. In such cases, coordination with the University's Physical Development Division (PDD) is required to ensure that the facility is not prone to natural and man-made hazards.

c) Access Procedure of Authorized Personnel

Directors or heads of a particular unit of the University shall have full control over who are allowed access to the data storage facility of their unit. A standard access procedure document template shall be agreed upon and released by the University Data Privacy Review team. This shall be used by the heads of office in detailing the access privileges of their unit's personnel and the mechanism by which other personnel may be granted access to the data storage facility. The access procedure document must be validated and approved by the DPO.

d) Documentation of Access

Authorized access to stored personal information must be documented in a format that allows monitoring of the name of personnel who accessed retained personal information and the date, time, duration and purpose of access.

e) Physical Location and Layout of Office or Data Facility

The Office of the DPO shall coordinate with the PDD to ensure that the location of critical data server facilities are not susceptible to natural and/or man-made hazards that may compromise the availability, integrity, and/or confidentiality of the stored data.

At the office level, computers should be positioned with considerable spaces between them to maintain privacy and protect the processing of personal information.

3. Technical Security Measures

1. Implementing Intrusion Detection Systems

All University-affiliated computer units that are part of the University's local area network or intranet shall be installed with an anti-virus software. As part of its IT Governance Framework, the University shall ensure that a network firewall is in place to secure the University's information systems and database against network-related attacks. The KMSD shall regularly check the firewall logs to monitor the University network for suspicious activities or security breaches.

2. Implementing Data Backup Procedure

The KMSD shall ensure that routine backup operations are performed. Full backups shall be done at least once a day while differential backups shall be done as frequent as necessary and applicable. Data backup facilities shall be remotely located from the actual data servers. For instance, a University campus may place its backup facility in one of the other campuses of the University. Data backup facilities may be moved to another location upon the advice of the KMSD and/or the PDD and the approval of the University President.

3. Encryption of Personal information

Digital documents containing sensitive personal information shall be encrypted using any of the standard encryption algorithms used in the field of information security during storage and while in transit.

4. Evaluating Software Applications

a. Whenever applicable, the KMSD shall evaluate and review software applications before they are installed on University computers or devices connected to the University network. This ensures that all software applications used by the University are compatible with the data privacy policies set in this Manual and in the Data Privacy Act of 2012.

b. In cases wherein software applications are installed without prior evaluation (e.g. application is already installed prior to the official adoption of this Manual), the KMSD shall perform the software evaluation during scheduled IT maintenance activities.

c. If a software application is determined to be a security risk, the technical personnel who performed the evaluation shall notify the end user of the risk before uninstalling the software application. The personnel should document the activity in an incident report.

5. Conducting Regular Assessment or Testing of Security Controls

To ensure that all the technical security controls implemented are working as intended, the University shall conduct vulnerability assessments and perform penetration testing on critical systems such as the University's network firewall and information systems periodically. The KMSD shall lead in the conduct of such tests.

PART 9. BREACH AND SECURITY INCIDENTS

1. Creation of a Data Breach Response Team

A Data Breach Response Team comprised of the DPO, Chief Administrative Officer (CAO), and the KMSD, under the direct supervision of the Vice-President for Planning, Quality Assurance, and Resource Management (PQuARM) is responsible for ensuring immediate action in the event of a security incident or Personal information breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

2. Measures to Prevent and Minimize Occurrence of Breach and Security Incidents

The Data Breach Response Team shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and to monitor for security breaches. The KMSD shall also conduct regular vulnerability scanning of computer networks. Personnel directly involved in the processing of Personal information shall attend trainings and seminars for capacity building. Periodic review of policies and procedures shall also be implemented.

3. Incident Response Procedure

Any suspected or actual security incident or Personal information breach must be reported immediately to any member of the Data Breach Response Team. The Team member shall then conduct an initial assessment of the reported incident or breach in order to ascertain the veracity, nature, and extent thereof. If the report is verified, the DPO shall convene all members of the Data Breach Response Team to discuss the implementation of the Incident Response Procedure to address the incident. The Team shall execute measures based on the conducted Privacy Impact Assessment to mitigate the adverse effects of the incident. Regardless of the type of incident, the general steps of the IRP are as follows:

i. Contain the security incident;
ii. Restore integrity to the affected information systems; and
iii. Mitigate possible harm or negative consequences

4. Notification Protocol

The DPO shall report the details of a data privacy breach to the National Privacy Commission (NPC) and the data subjects affected within 72 hours from knowledge thereof.

5. Documentation and Reporting Procedure of a Data Privacy Breach

The Data Breach Response Team shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to the Vice-President for Administration, University President, and the NPC within the prescribed period. The report shall contain the following:

a. Description of the nature of the breach;
b. Personal information possibly involved;
c. Measures undertaken by the team to address the breach and reduce the harm or its negative consequences; and
d. Names of the personal information controller, including contact details, from whom the data subject can obtain additional information about the breach and any assistance to be provided to the affected data subjects.

PART 10. INQUIRIES AND COMPLAINTS

1. Inquiries

The office of the DPO shall provide channels of communication, both physical and digital, between the DPO and the data subjects. Data subjects may write an e-mail to the office of the DPO to request for information on matters relating to the processing of their Personal information under the custody of the University. Alternatively, they may visit the office of the DPO to submit a printed copy of their letter of inquiry with their contact details for reference.

2. Complaints

Complaints shall be filed in three (3) printed copies to the Office of the DPO or sent electronically to same Office's official e-mail address. The Office shall confirm with the complainant its receipt of the complaint. Upon validation of the complaint, the DPO shall initiate the conduct of an official internal investigation. The results of the investigation shall be reported to the NPC within seventy-two (72) hours from the official knowledge of the Personal information breach.

PART 11. REPEALING CLAUSE

Any other University issuance, memorandum, rule or regulation and/or parts thereof contrary to or inconsistent with the provisions of this Manual is hereby repealed, modified or amended accordingly.

PART 12. SEPARABILITY CLAUSE

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

PART 13. EFFECTIVITY

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

PART 14. ANNEXES

Annex A

University of Southeastern Philippines's Data Privacy Statement

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

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

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

What Personal information the University may collect and process?

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

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

- Name
- Specimen signatures
- Home address
- Email address
- Biographical information
- Academic information
- Nationality
- Phone number
- Government or Non-government Identification Number / Card
- Financial information
- Employment details

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

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

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

Why does the University collect and process Personal information?

The purpose of Personal information collection and processing may vary from one University procedure (e.g. student admission, visitor entry, human resource management, etc.) to another. However, the general principle governing the University's data collection process is legitimacy of purpose.

The University shall only collect and process data for legitimate purposes in consonance with its inherent functions and in compliance with legal requirements. These legitimate purposes may include, but may not be limited to, the following:

- To verify students' and employees' identity;
- To generate statistics and analytics useful for administrative decisions;
- To strengthen security measures and facilitate investigations of reported violations;
- To easily generate statutory reports;
- For employee and human resources management purposes (as may be required by applicable laws);
- For research purposes or endeavors contributing to the body of knowledge;
- To comply with legal or regulatory obligations;
- To establish, exercise or defend legal claims

How does the University share or disclose Personal information?

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

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

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

How does the University protect Personal information?

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

How long does the University retain Personal information?

Personal information are retained only for as long as necessary to serve its declared purpose or comply with regulatory and legal requirements. Depending on the nature of data and purpose it serves, the retention period could range from days (e.g. CCTV recording) to years (e.g. student academic information). Whenever retention becomes unnecessary, the University shall dispose the Personal information properly through a secure and confidential means.

Annex B

CONSENT FORM

I have read the University of Southeastern Philippines' Data Privacy Statement and hereby allow the University to collect, use, process and store my personal information through its official channels for legitimate purposes.

I affirm my fundamental right to privacy and my constitutional data privacy rights as stated in the Republic Act No. 10173 of the Philippines. This consent is hereby given on the guarantee that these rights shall be upheld at all times.

_____

Data Subject Signature over Printed Name

Annex C

Data Security and Privacy Risk Management Matrix

Risk Rating = Probability x Impact

I. Collection

Quality Objective: To foresee all possible general risks inherent in the collection of Personal information and to identify the appropriate and reasonable preventive and mitigating measures that would address these risks.

ID	RELATED RISKS	LIKELIHOOD	SEVERITY	RISK FACTOR	CONTROLS/MITIGATION
C01	Inaccuracy of collected data resulting from data entry errors.	Low (1)	Low (1)	1	**Preventive:** Implement data entry policies, automated and/or manual, to lessen the possibility of data inaccuracy. This may include, but not limited to, the following actions: • Incorporate automated mechanisms or algorithms that: force the encoder to review or confirm the encoded data; and also check syntactical, formatting, and data type mismatch errors. • Define a comprehensive and well-documented data collection policy and protocol that should include provisions regarding general steps, automated or manual, to perform to promote data accuracy. This may include: review and confirmation. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature. Specifically, this may entail the implementation of a data rectification and deletion procedure that should involve the

					process owners, development team, data privacy team, and top management.
C02	Collection of data from the data subject without the data subject's explicit consent.	Low (1)	Low (1)	1	**Preventive:** Specify clearly in the user agreement statement the data to be collected and the manner by which they will be acquired. A data privacy review team must regularly oversee and supervise the data collection process through a set of detective controls which may include or be a combination of: process, human capital, physical, and/or technological controls. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.
C03	Use of Internet or local network cookies without prior consent to collect relevant online information pertaining to the data subject; and/or monitor the data subject's online activity.	Low (1)	Low (1)	1	**Preventive:** Establish a quality assurance and code review team, as specified in the official data privacy policy manual, to oversee the development and review the source code of official University websites and applications and, coordinate with the data privacy review team for determining parts and functions that concern an individual's rights to privacy and the steps to perform to uphold these rights. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.

C04	Inadvertent public disclosure of sensitive Personal information during data collection.	Low (1)	High (3)	3	**Preventive:** Define a comprehensive and well-documented data collection policy and protocol that should include provisions regarding the required setting, context, mechanisms, and conditions that should be present in order for the collection of sensitive Personal information to commence without compromising the individual's right to privacy. A data privacy review team must be established to regularly oversee and audit the implementation of these policies. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.
C05	Unauthorized collection of data subject data by an unauthorized system and/or personnel, internal or external to the institution. Specifically, this may include but not limited to the following actions: • Data collection caused by a system breach. • Data collection induced by	Medium (2)	High (3)	6	**Preventive:** Define a comprehensive and well-documented data collection policy and protocol that should include provisions regarding process ownership, access rights and user privileges for each legitimate University applications and processes. A data privacy review team must be established to regularly audit the implementation of these policies and oversee the data collection process through a set of detective controls which may include or be a combination of: process, human capital, physical, and/or technological controls. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.

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

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

II. Use

Quality objective: To foresee all possible general risks inherent in the use of Personal information and to identify the appropriate and reasonable preventive and mitigating measures that would address these risks.

ID	RELATED RISKS	LIKELIHOOD	SEVERITY	RISK FACTOR	CONTROLS/MITIGATION
U01	Processing of collected data for purposes not explicitly stated in the user agreement statement.	Low (1)	Medium (2)	2	**Preventive:** Specify clearly in the user agreement statement the scope and extent to which the collected data will be reasonably used; and, establish a data privacy review team that regularly oversee and supervise the processing of data through a set of detective controls which may include or be a combination of: process, human capital, physical, and/or technological controls. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and

					document the incident for purposes of investigation and prevention of future incidents of the same nature.
U02	Unauthorized processing of data subject data by an unauthorized system and/or personnel internal or external to the institution.	Medium (2)	High (3)	6	**Preventive:** Define a comprehensive and well-documented acceptable data use policy that should include provisions regarding process ownership, access rights and user privileges for each legitimate University applications and processes. A data privacy review team must be established to regularly oversee and supervise the processing of data through a set of detective controls which may include or be a combination of: process, human capital, physical, and/or technological controls. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature. (Trail audits, system logs)
U03	Use of personal and/or sensitive information with malicious intent.	Medium (2)	High (3)	6	**Preventive:** Define a comprehensive and well-documented acceptable data use policy that should include provisions regarding the practice of due diligence when dealing with personal information. A data privacy review team must be established to regularly oversee and supervise the processing of data through a set of detective controls which may include or be a combination of: process, human capital, physical, and/or technological controls.

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

III. **Retention**

Quality Objective: To foresee all possible general risks inherent in the retention of Personal information and to identify the appropriate and reasonable preventive and mitigating measures that would address these risks.

ID	RELATED RISKS	LIKELIHOOD	SEVERITY	RISK FACTOR	CONTROLS/MITIGATION
R01	Storage and retention of Personal information irrelevant to the institution's functions.	Low (1)	Medium (2)	2	**Preventive:** Define a comprehensive and well-documented data retention policy that should include the following provisions: • Coordination of process owners, users, development team, top management, and the data privacy review team to determine reasonable data to collect and store for a given process or application. • Regular monitoring and overseeing of retained data through a set of detective controls which may include or be a combination of: process, human capital, physical, and/or technological controls. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.

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

					rights and user privileges for each legitimate University applications and processes. A data privacy review team must regularly oversee and audit the implementation of these policies. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature. (Regular trail audits)
R04	Irrelevant, redundant, outdated, or unnecessary data hogs space in the institution's data storage facility.	Low (1)	Medium (2)	2	**Preventive:** Define a comprehensive and well-documented data retention policy that should include the following provisions: • Coordination of development, quality assurance, and data privacy review teams to ensure that controls and measures are in place to guarantee the accuracy and currency of retained data especially in systems involving a centralized database. • Regular monitoring and overseeing of retained data through a set of detective controls which may include or be a combination of: process, human capital, physical, and/or technological controls. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and

					appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature. Specifically, This may entail the implementation of a data rectification and deletion procedure that should involve the process owners, development team, data privacy team, and top management.

IV. Disclosure

Quality Objective: To foresee all possible general risks inherent in the disclosure of Personal information and to identify the appropriate and reasonable preventive and mitigating measures that would address these risks.

ID	Risk			Risk Rating	Measures
DE01	Disclosure of data, raw or derived, for unreasonable purposes to benefit or damage parties external to the institution	Low (2)	High (3)	6	**Preventive:** • Specify clearly in the user agreement statement the scope and extent to which the collected data will be reasonably disclosed • Establish a data privacy review team that ensure the practice of due diligence when disclosing data • Establish a data privacy review team that regularly oversee and supervise the disclosure of data through a set of detective controls which may include or be a combination of: process, human capital, physical, and/or technological controls. **Mitigating:**

					Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.
DE02	Unauthorized disclosure of data by an unauthorized system and/or personnel internal or external to the institution.	Medium (2)	High (3)	6	**Preventive:** Define a comprehensive and well-documented data disclosure policy and protocol that should include provisions regarding process ownership, access rights and user privileges for each legitimate University applications and processes. A data privacy review team must be established to regularly oversee and audit the implementation of these policies. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.
DE03	Disclosure of collected data for purposes not explicitly stated in the user agreement statement.	Medium (2)	High (3)	6	**Preventive:** Specify clearly in the user agreement statement the scope and extent to which the collected data will be reasonably disclosed; and, establish a data privacy review team that regularly oversee and supervise the disclosure of data through a set of detective controls which may include or be a

					combination of: process, human capital, physical, and/or technological controls. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or mitigate the inherent adverse effects of the incident; determine the person/s liable; and document the incident for purposes of investigation and prevention of future incidents of the same nature.

III. Disposal

Quality objective: To foresee all possible general risks inherent in the disposal of Personal information and to identify the appropriate and reasonable preventive and mitigating measures that would address these risks.

ID	RELATED RISKS	LIKELIHOOD	SEVERITY	RISK FACTOR	CONTROLS/MITIGATION
DL01	Personal and sensitive information stored in decommissioned storage devices remain intact, making them susceptible to unauthorized access	Medium (2)	High (3)	6	**Preventive:** Define a comprehensive and well-documented data disposal policy and protocol. This policy may include, but not limited to, the following provisions: • Deep formatting of storage devices before decommissioning to remove stored data • Perform relevant measures to prevent unauthorized data recovery. **Mitigating:** Implement a data privacy incident response procedure, as specified in the official data privacy policy manual, to ensure that timely and appropriate action is taken to contain and/or

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

Definition

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

- An action plan is required for risk factor ≥5