THE CPSU DATA PRIVACY MANUAL

PART 1 BACKGROUND

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

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

The law ensures that entities or organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights. The law serves the following purposes:

1. Protects the privacy of individuals while ensuring free flow of information to promote innovation and growth;

2. Regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data; and

3. Ensures that the Philippines complies with international standards set for data protection through the NPC.

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

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

PART 2 INTRODUCTION

This Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and other relevant policies, including issuances of the National Privacy Commission.

It is the policy of Central Philippines State University (CPSU) to respect and uphold data privacy rights, and to ensure that all personal data collected from students, their parents or guardians, employees and other third parties, are processed pursuant to the general principles of transparency, legitimate purpose, and proportionality as stated in DPA.

This Manual outlines the data protection and security measures adopted by the University to protect data.

PART 3 DEFINITION OF TERMS

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

b. *Data Sharing* – refers to the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor.

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

d. *Personal Data* – refers to all types of personal information.

e. *Personal Data Breach* – refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

f. *Personal Information* – refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

g. *Personal Information Controller (PIC)* – refers to an official/personnel who controls the collection, holding, processing, use, transfer, or disclosure of personal information, including an official/personnel who instructs another official/personnel to collect, hold, process, use, transfer or disclose personal information on his/her behalf. There is control if the official/personnel decides on what information is collected, or the purpose or extent of its processing. The term excludes an official/personnel who performs such functions as instructed by another official/personnel, and an official/personnel who collects, holds, processes, uses, transfers or discloses personal information in connection with the individual's personal, family or household affairs.

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

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

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

k. *Sensitive Personal Information* – refers to personal information:

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

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

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

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

PART 4 SCOPE AND LIMITATIONS

Section 1. Scope

All officials, employees, and staff of the University, whether regular, contractual, or project-based, who are engaged in processing personal information on any of its campuses, offices, or departments are subject to the provisions of this manual.

The employees or people of the University are intended to utilize and apply this manual, which is basically an internal issuance. No of their form of employment or contractual arrangement, all University employees are required to abide by the rules outlined in this Manual.

Section 2. Limitations

The following do not apply to this manual:

a. Information pertaining to a person's job or duties concerning anybody who is or was a government institution employee or official, including:

   i. the person's status as a current or former official or employee of a government organization;

   ii. the person's name, place of business, and contact information for the office;

   iii. the job title, pay scale, and duties of the individual's current employment; and

   iv. the name of the person appearing on a document they created while working for the government;

b. information on a person who is or was doing work for a government institution under contract, but only insofar as it related to that work, including the person's identity and the conditions of their contract;

c. Information about a financial benefit awarded to a person at the government's discretion, such as the granting of a license or permit, including the recipient's name and the precise nature of the benefit, provided that they do not include rewards received out of the ordinary course of business or as a matter of right;

PART 5. DATA PRIVACY PRINCIPLES

The University gathers basic contact information from its students, graduates, staff, personnel, suppliers, contractors, consultants, and other customers over the course of its operations, including, among other things, their complete name, address, email address, and phone number. The University will use the collected personal data, among

other things, for communication, recording, and documentation reasons. The University shall make sure that any personal data in its possession is safeguarded against any unintentional or accidental loss, modification, or disclosure, as well as from any other illegal processing.

Even after resignation, contract termination, or other contractual ties, all University employees and staff are required to protect the confidentiality and secrecy of any personal data that comes into their knowledge and control. Only legitimate purposes and authorized recipients may receive personal information held by the University in its possession.

Section 1. Principles of Transparency, Legitimate Purpose and Proportionality

Processing of personal data is permitted, provided that it complies with this Manual's standards, other laws that permit dissemination of information to the public, and the principles of openness, lawfulness, and proportionality:

a. *Transparency* – The subject of the personal data must be aware of the scope, nature, dangers, and protections associated in the processing of his or her data, as well as his or her rights as a data subject and how to exercise those rights. All communications and information pertaining to the processing of personal data should be simple to comprehend and easy to obtain.

b. *Legitimate Purpose* – Information processing must be in line with a clearly stated goal that doesn't violate morality, the law, or public policy.

c. *Proportionality* – In respect to a stated and agreed-upon objective, information processing must be sufficient, relevant, appropriate, required, and not excessive. Only when no other reasonable method could reasonably be used to achieve the processing goal may personal data be processed.

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

The following broad principles must be followed in the collection, processing, and storage of personal data:

a. The objective of collection must be clearly stated, specific, and legal.

    i. With the exception of the exceptions set out in this Manual and other relevant laws and regulations, consent is necessary prior to the collection and processing of personal data. When permission is needed, it must be limited in time in relation to the declared, stated, and legal purpose. Given consent may be revoked.

    ii. The aim and scope of processing, including, if applicable, the automated processing of the data subject's personal information for

profiling or data sharing, must be made explicitly known to the data subject.

iii. Prior to collecting or as soon as is practically possible following, the purpose must be decided upon and proclaimed.

iv. Only required personal information that is consistent with the stated, indicated, and legal purposes may be gathered.

b. Personal information must be handled honestly and legally:

i. The right of the data subject to reject, revoke consent, or object must be respected throughout processing. It must also be clear and provide the data subject enough information to understand the kind and scope of processing.

ii. To make sure that they are simple to understand and access, all information sent to a data subject must always be written in clear, simple language.

iii. Processing must be done in a way that is consistent with the stated, agreed-upon, and legal purpose.

iv. Personal data that is processed should be sufficient, relevant, and restricted to what is required in connection to the purposes for which it is processed.

v. Processing must be done in a way that guarantees the necessary security and privacy precautions.

c. Processing ought to guarantee data integrity:

i. When essential for a stated, explicit, and legal purpose, personal data should be accurate and kept up to date.

ii. Correcting, completing, destroying, or restricting further processing of inaccurate or incomplete data is required.

d. No personal information should be kept longer than is required.

i. Personal data must only be kept as long as is required.

• to achieve the stated, acknowledged, and lawful purpose, or after the necessary processing for the purpose has been completed;

• for the purpose of establishing, asserting, or defending legal claims; or

• for lawful business objectives, which must be compliant with industry standards or authorized by the relevant government agency.

ii. Retention of personal data shall be allowed in cases provided by law.

iii. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.

e. Any approved future processing must have sufficient security measures:

i. Subject to the implementation of the necessary organizational, physical, and technical security measures required by the DPA in order to safeguard the rights and freedoms of the data subject, personal data that was initially collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes and, in cases specified by law, may be stored for longer periods of time.

ii. The retention of personal data that is aggregated or retained in a format that prevents data subjects from being identified may go beyond what is required for the stated, indicated, and lawful purpose.

iii. No personal information must be kept indefinitely with the intention of some unspecified potential use in the future.

Section 3. General Principles for Data Sharing

Under any of the following circumstances, further processing of personal data obtained from a source other than the data subject is permitted:

a. Data sharing is permitted when it is specifically permitted by law, provided that there are sufficient protections for data security and privacy and that processing complies with the principles of openness, necessity, and proportionality.

b. When personal information about a data subject is publicly available or has the consent of the data subject, data collected from parties other than the data

subject for research purposes is permitted, provided that adequate safeguards are in place and no decision directly affecting the data subject is made on the basis of the data collected or processed. In order to protect data subject rights, research integrity must not be jeopardized.

c. A Data Sharing Agreement must be in place before any government entities may share data for the benefit of a public function or the delivery of a public service.

PART 6. PROCESSING OF PERSONAL DATA

Section 1. Lawful Processing of Personal Information

Processing of personal data is permitted unless specifically forbidden by law. Any of the following prerequisites must be met for processing to be legitimate:

a. Before the data is collected, or as soon as is feasible and reasonable after, the data subject must have provided consent;

b. Personal information of a data subject who is a party to a contract is processed in order to carry out contractual duties or to take action at the request of the data subject before joining the contract;

c. The personal information controller must treat the data in order to comply with a legal requirement;

d. The protection of the data subject's essential interests, including his or her life and health, necessitates the processing;

e. Processing of personal data is required by law to react to a national emergency or to uphold the needs of public order and safety;

f. A public authority's constitutional or legislative obligation requires the processing of personal information to be carried out; or

g. The processing is required to further the PIC's or the party or parties to whom the data has been supplied, unless such interests are outweighed by the data subject's basic rights and freedoms, which are protected by the Constitution.

Section 2. Sensitive Personal and Privileged Information

Except for the circumstances listed below, processing of sensitive personal information is forbidden.

a. Prior to the processing of sensitive personal information or privileged information, which shall be carried out for a stated, defined, and legitimate

purpose, consent is obtained from the data subject or from the parties to the exchange of privileged information.

b. Existing rules and regulations permit the processing of highly sensitive personal data or privileged information, provided that they do not impose a need for the data subject's permission and ensure the protection of personal information.

c. The data subject is not physically or legally competent to provide his or her permission before the processing because it is essential to safeguard the data subject's life and health or the life and health of another person;

d. The processing is required in order for public organizations and their associations to fulfill their legitimate and nonprofit goals, provided that:

    i. It is restricted to and relates to the actual members of these organizations or their associates;

    ii. The transmission of sensitive personal data to third parties is prohibited; and

    iii. obtaining the data subject's consent before processing;

e. The processing is required for the purpose of providing medical care if: (a) it is done by a medical professional or a facility that provides medical care, and (b) a sufficient degree of personal data protection is guaranteed; or

f. As part of the establishment, exercise, or defense of legal claims, or when provided to government or public authority in accordance with a constitutional or statutory mandate, the processing relates to sensitive personal information or privileged information that is necessary to protect the legal rights and interests of natural or legal persons in court proceedings.

Section 3. Extension of Privileged Communication

a. PICs may use the privileged communication principle in relation to privileged information that they legitimately hold or process. Any evidence derived from privileged knowledge is inadmissible, subject to applicable rules and regulations.

PART 7. SECURITY MEASURES

Section 1. Data Privacy and Security

Aiming to prevent both natural threats like accidental loss or destruction and human threats like unauthorized access, fraudulent use, unauthorized destruction, modification,

and infection, security measures are meant to safeguard the accessibility, integrity, and confidentiality of personal data.

To safeguard personal information, PIC and PIP must put in place reasonable and suitable organizational, physical, and technological security measures. The PIC and PIP must take precautions to make sure that any individual operating on their behalf who is a natural person and has access to personal data does not handle it without their permission or in accordance with legal requirements.

The security measures should be designed to prevent any accidental or unauthorized destruction, modification, or disclosure of personal data, as well as against any other illegal processing, and to safeguard the availability, integrity, and confidentiality of personal data. These safeguards must be put in place to guard against both natural hazards like accidental loss or destruction and human hazards such unauthorized access, fraudulent use, wrongful destruction, modification, and contamination.

Section 2. Organizational Security Measures

At least once each year, the University is required to provide a training session on data security and privacy. Management is responsible for ensuring the presence and involvement of staff members who are directly engaged in the processing of personal data at all mandatory orientations and training sessions.

Every project, activity, and system that involves the processing of personal data must undergo a Privacy Impact Assessment (PIA) by the university. It may decide to hire a third party to carry out a PIA on its behalf. A non-disclosure agreement will be required of each employee.

Employees who have access to personal information are required to treat it with absolute secrecy if it is not intended for public exposure.

Annual reviews and evaluations of this manual are required. To maintain compliant with current data privacy best practices, privacy and security policies and procedures at the university must be updated.

The following recommendations for organizational security must be followed, if applicable, by PIC and PIP:

a. *Compliance Officer* – The University shall designate a person or persons to serve as the Data Protection Officer (DPO). The following duties and obligations belong to the DPO:

    i. observe how the PIC and PIP adhere to the DPA, its IRR, the NPC's issuances, and other relevant laws and rules;

ii. execute a privacy impact assessment (PIA) in relation to the PIC or PIP's actions, measures, initiatives, programs, or systems;

iii. Inform the PIC or PIP of complaints or the exercise of rights by data subjects;

iv. Make sure the PIC or PIP manages security incidents and data breaches properly, making ensuring the latter prepares and submits reports and other documentation about security incidents or data breaches to the NPC within the allotted time;

v. Educate and promote understanding of privacy and data protection issues within the University, including all relevant laws, directives, and NPC issuances;

vi. Promote the creation, evaluation, and/or updating of PIC or PIP privacy and data protection policies, guidelines, initiatives, and/or programs by using a privacy by design methodology;

vii. serve as the PIC or PIP's point of contact for any inquiries about data privacy or security concerns or problems with data subjects, the NPC, and other authorities;

viii. cooperate, plan, and consult the NPC on issues pertaining to data privacy and security;

ix. do any additional activities or obligations that the PIC or PIP may assign in order to advance the interests of data privacy and security and safeguard the rights of data subjects;

x. take charge of adhering to the NPC's registration and compliance requirements as outlined in the DPA and its IRR, including the registration of systems for processing personal data, notifying the DPA of automated processing operations when appropriate, and submitting an annual report of the summary of security incidents and data breaches that have been documented;

xi. The permission form, access request form, request for rectification or erasure form, and privacy notifications should be recommended for approval.

b. *Conduct of Trainings/Seminars* – At least once per year, the University must provide a required lecture on data privacy and security. Management must make sure that employees who are directly engaged in the processing of personal data attend and take part in relevant orientations and training sessions as frequently as required.

c. *Conduct of Privacy Impact Assessment (PIA*) – For every project, activity, and system that involves the processing of personal data, the University is required to complete a Privacy Impact Assessment (PIA). It might decide to entrust a third party with carrying out a PIA.

d. *Data Protection Policies* – Any individual or organization—natural or legal—involved in the processing of personal data is required to put in place appropriate data protection policies that address organizational, physical, and technical security measures while also taking into account the risks to the rights and liberties of data subjects. The CPSU Data Privacy Manual Page 16 of 29.

    i. The policies must put data protection principles into practice both when deciding on the methods of processing and when processing is actually taking place.

    ii. The rules must put in place the essential security measures that, by default, guarantee that only personal data that is required for the specific processing purpose is handled. They are responsible for deciding how much personal information is gathered, how it is processed, how long it is stored, and how easily it is accessible.

    iii. The rules must outline how privacy and security policies and procedures will be documented, regularly reviewed, assessed, and updated.

e. *Records of Processing Activities* – Any natural or legal person, as well as any other organization, participating in the processing of personal data must keep documents that adequately define the system used to handle the data and list the responsibilities of those who will have access to it. Records should contain:

    i. details on the motivations for the processing of personal data, including any foreseeable future processing or data exchange;

    ii. a description of each kind of data subject, each receiver of their personal information, and how they will be used;

    iii. general details regarding the flow of data through the business, including the duration of data collection, processing, and retention as well as the deadlines for personal data deletion or disposal;

iv. a summary of the organizational, physical, and technology security measures in place;

v. The name and contact information of the PIC, and, if applicable, the joint controller, its representative, the compliance officer or DPO, or any other individual or individuals responsible for ensuring compliance with the relevant laws and regulations for the protection of data privacy and security.

f. *Management of Human Resources* – Selecting and managing its employees, agents, or representatives, especially those who will have access to personal data, is the responsibility of every natural or legal person or other organization engaged in the processing of personal data. It will be necessary for the staff members to sign a non-disclosure agreement. If personal information is not meant for public exposure, all workers, agents, or representatives having access to it must maintain strict secrecy. The CPSU Data Privacy Manual Page 17 of 29 Even after leaving the public service, changing jobs, or ending their employment or contractual relationships, they are still obligated to fulfill this responsibility. For these workers, agents, or representatives, there must be capacity-building, orientation, or training programs respecting privacy or security rules.

g. *Processing of Personal Data* - Any individual or entity that processes personal data must create, put into practice, and evaluate the following:

i. a method for gathering personal information, which should include steps for gaining permission when necessary;

ii. procedures that restrict data processing to guarantee that it only occurs as needed to achieve the stated, stipulated, and lawful goal;

iii. policies for access control, system monitoring, and procedures to adhere to in the event of a security incident or technical issue;

iv. guidelines and processes for data subjects to exercise their DPA rights;

v. A data retention schedule that outlines the timeframe or requirements for erasing or discarding documents.

h. Contracts with Personal Information Processors (PIP) – The PIC should guarantee that its PIPs, when relevant, implement the security measures required by this Manual by means of the necessary contractual arrangements. It must only work with PIPs that provide strong enough assurances to execute the necessary security measures outlined in this Manual and guarantee the protection of data subjects' rights.

i. Review of Privacy Manual – Every year, this manual will be reviewed and assessed. The University's privacy and security policies and procedures must be updated to be compliant with current data privacy best practices.

Section 3. Physical Security Measures

Physical security measures are designed to keep an eye on and restrict access to the location that houses the personal data, as well as the activities that take place there. They cover things like the facility's real layout, the positioning of furniture and equipment, approved transfer methods, and the duration, methods, and timeline for data preservation and destruction, among other things.

The following must be followed in order to guarantee that mechanical destruction, manipulation, and modification of personal data in the University's custody are prohibited, as well as that these data are safeguarded from external access, man-made catastrophes, power outages, and other similar threats:

a. Both paper-based/physical and digital/electronic formats of personal data must be kept by the university.

b. The University is required to keep all personal data it processes in a data room where paper documents are preserved in lockable filing cabinets and digital/electronic files are saved on computers.

c. The data room may only be accessed by authorized staff. They will each get a duplicate key to the room for this use. Upon submitting an access request form to the DPO and receiving his or her permission, other staff may be given access to the room.

d. All individuals who are permitted to enter and use the data room or facility must register online using the university's registration system and fill out a logbook that is kept beside the door. They must state the day, hour, length, and reason for each access.

e. To secure processing of personal data and guarantee privacy, the computers are placed with a lot of distance between them.

f. The confidentiality and integrity of personal data must always be maintained by those who are engaged in processing. When entering the data storage area, they are not permitted to bring any of their own devices or storage devices.

g. Personal data transfers through email must be done through a secure email service that encrypts the data, including any and all attachments. Documents containing personal data may not be sent using facsimile technology.

h. The University must keep a client's or customer's personal information for a certain period of time after acquisition. All hard copies and digital copies of the personal data must be deleted when the specified time limit has passed and disposed of safely.

The following rules for physical security must be followed by PICs and PIPs as necessary:

a. Policies and procedures, particularly those that outline the correct use of and access to electronic media, must be put into place in order to monitor and regulate access to and activities in the room, workstation, or facility;

b. When designing office space and workstations, keeping the surroundings and the general public's accessibility in mind, privacy must be provided to anybody processing personal data, including the physical layout of furniture and equipment;

c. To guarantee that only those performing official activities are present in the space or at the workstation at any one time, the roles, responsibilities, and timetable of those engaged in processing personal data must be clearly specified;

d. Implementing policies and procedures addressing the transfer, removal, destruction, and re-use of electronic media is required for every natural or legal person, as well as any other entity, engaged in the processing of personal data;

e. It is necessary to develop policies and processes that stop the mechanical destruction of documents and equipment. As far as is practical, the area and workstation used to handle personal data must be protected against calamities, power outages, unauthorized access, and other similar dangers.

Section 4. Guidelines for Technical Security Measures

Each PIC and PIP must put in place technical security measures, such as encryption and authentication procedures that regulate and limit access, to ensure that there are enough and suitable safeguards to protect the processing of personal data, notably the computer network in place:

a. The University must monitor security lapses and notify the organization of any attempts to disrupt or interrupt the system using an intrusion detection system.

b. To ensure that security measures are compatible with overall operations, the University must first assess and evaluate software programs before installing them in computers and other devices used by the organization.

c. The University must regularly evaluate security policies, carry out vulnerability analyses, and carry out penetration testing throughout the organization as directed by the relevant department or unit.

d. Each employee who has access to a person's personal information must use multi-level authentication and a secure encrypted connection to prove their identity.

e. In the case of a security incident or breach of personal data, a Data Breach Response Officer (DBRO) will be in charge of making sure that appropriate action is taken right away. To determine the nature and scope of the event or breach, the DBRO should perform an initial evaluation. Additionally, he or she must put plans in place to lessen the consequences of the event or breach.

f. The University must undertake PIAs on a regular basis to pinpoint processing system hazards, keep an eye out for security lapses, and scan computer networks for vulnerabilities. It is required that employees who work directly with personal data process them undergo trainings and seminars to develop their skills. The CPSU Data Privacy Manual Page 20 of 29 Periodic reviews of the University's policies and practices are also required.

g. All personally identifiable information that is in the University's care must always be kept in a backup file. It must constantly compare the backup with the impacted file in the case of a security incident or data breach to check for any discrepancies or modifications brought on by the incident or breach.

h. The management will be made aware by the DBRO of the obligation to notify the NPC and any impacted data subjects within the legally required time frame. The DBRO may get the real notice if Management so chooses.

i. Every event or breach that occurs must be thoroughly documented by the DBRO, along with an annual report that must be sent in to management and the NPC within the allotted time frame.

The following technological security measures must be adopted and established by PICs and PIPs as necessary:

a. a security protocol for the handling of personal data;

b. protection measures for their computer network against unintentional, illegal, or unauthorized use, any interference that might compromise data integrity or impair the system's availability, and unauthorised access over an electronic network;

c. the capacity to guarantee and maintain the integrity, availability, confidentiality, and robustness of their processing systems and services;

d. a method for discovering and accessing reasonably anticipated vulnerabilities in their computer networks, as well as for taking preventative, corrective, and mitigating action against security events that may result in a breach of personal data; regular monitoring for security breaches;

e. the capacity to swiftly recover access to and availability of personal data after a technological or physical incident;

f. a procedure for routinely testing, analyzing, and reporting on the performance of security controls;

g. Personal data encryption during storage and transmission, the authentication procedure, and other technological security measures that regulate and restrict access.

PART 8. SECURITY OF SENSITIVE PERSONAL INFORMATION

As far as is practical, the University must employ the most suitable standard recognized by the ICT sector to safeguard any sensitive personal data kept by it.

Section 1. Access to Sensitive Personal Information

On-Site and Online Access:

a. On government property or via online resources, no government employee should have access to sensitive personal data unless the University, the organization that first gathered the data, has granted them a security clearance.

b. The University must tightly restrict who has access to sensitive personal data that is in its care or under its management, especially if online access is permitted. Only when access to the personal data is necessary for an employee of the government to carry out their duties or provide a public service that is directly dependent on it will they be given a security clearance.

c. Online access to sensitive personal information should be subject to the following restrictions, except as provided in the next previous paragraphs:

    i. Design and implementation of an IT governance framework;

    ii. the establishment of adequate organizational, physical, and technological security measures;

    iii. The organization may safeguard sensitive personal data in line with accepted information and communication technology (ICT) industry data privacy practices and standards;

iv. Only the sensitive personal information required for the execution of official duties or the delivery of a public service is made available to the government employee online.

Off-Site Access:

a. An agency's head must guarantee the adoption of privacy rules and suitable security measures before sensitive personal information kept by the agency is moved to or accessed from a place off or outside of government property, whether by its agent or employee. The director of the agency must receive and authorize any requests for such access or transportation. The request must include suitable accountability procedures for the data processing.

b. According to the following rules, the head of agency must accept requests for off-site access:

i. Time limit for approval or rejection. Within two (2) business days after the request's filing date, the head of the agency must accept or reject the request. The request is deemed rejected if the head of the agency does not take any action;

ii. Maximum of 1,000 Records. If a request is granted, the head of the agency must restrict access to no more than one thousand (1,000) documents at once, with the exception of the clause that follows.

iii. Encryption. Use of the most secure encryption must be utilized to protect any technology used to store, transfer, or access sensitive personal information for off-site access purposes and allowed under this paragraph.

PART 9. RIGHTS OF DATA SUBJECTS

Section 1. Rights of the Data Subject

The data subject is entitled to the following rights:

a. Right to be Informed

i. The data subject has a right to know if his or her personal information will be, is being, or has already been processed, including whether automated decision-making and profiling are being used.

ii. Before entering the data subject's personal information into the personal information controller's processing system, or at the earliest possible opportunity, the data subject shall be informed and provided with the information set out herein:

- Describe the personal information that has to be submitted into the system;
- its intended or current uses, which may include direct marketing, profiling, or historical, statistical, or scientific purposes;
- basis for processing, if the data subject's permission is not the basis for processing;
- the extent and procedure for processing personal data;
- The receivers or groups of recipients to whom the personal data have been shared or may be disclosed;
- methods used for automated access, whether the data subject has given permission for such access, and the scope of such authorization, including relevant details regarding the logic involved as well as the relevance and anticipated effects of such processing for the data subject;
- the name and contact information of the person in charge or a representative;
- the duration for which the data will be kept; and
- their ability to file a complaint with the NPC as well as their rights as data subjects, which include the right to access, rectify, and object to the processing of their personal data.

b. *Right to Object*. The processing of the data subject's personal information, including processing for direct marketing, automated processing, or profiling, may be objected to. In the event that any of the information provided or disclosed to the data subject in the previous paragraph changes, the data subject must also be informed and given the chance to withdraw permission to the processing.

The personal information controller must stop processing personal data when a data subject objects or withdraws permission, unless:

i. a subpoena requires the personal information;
ii. When it is necessary for the performance of or in connection with a contract or service to which the data subject is a party, or when it is necessary or desirable in the context of an employer-employee relationship between the collector and the data subject, among other obvious reasons for collection and processing;

iii. A legal need has led to the collection and processing of the data.

c. *Right to Access*. Upon request, the data subject has a right to reasonable access to the following:

i. the details of his or her processed personal data;

ii. sources where personal information was gathered;

iii. recipients' names and addresses for the personal data;

iv. the method used to process such data;

v. the justifications, if any, for disclosing the personal data to the recipients;

vi. information on computerized procedures when the data will, or is likely to, be the only basis for any decision that materially affects or will impact the data subject;

vii. Date of the latest access or modification to the data subject's personal information;

viii. The title, name, and/or address of the person in charge of handling your personal data.

d. *Right to Rectification*. Unless the request is frivolous or otherwise unjustified, the data subject has the right to contest any inaccuracy or mistake in the personal data and request that the PIC remedy it straight away. Provided, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject, the PIC shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof.

e. *Right to Erasure or Blocking*. The data subject has the right to request that his or her personal data be blocked, deleted, or otherwise removed from the PIC's file system.

i. If any of the following are discovered and sufficiently proven, this privilege may be exercised:

- The personal information is inaccurate, out-of-date, false, or was acquired illegally;
- Personal information is being used without the data subject's consent;
- The personal information is no longer required for the reasons it was originally obtained;
- there is no other legal basis or overriding legitimate interest for the processing, and the data subject withdraws consent or objects to the processing;

- The private information that the personal data relates to is damaging to the data subject, unless press, speech, or expression freedoms or other legal provisions make it acceptable;

- The processing is unauthorized.

- The rights of the data subject were breached by the PIC or PIP.

ii. The PIC may notify third parties who have previously received such processed personal information.

f. *Right to Damages.* Taking into consideration any violations of his or her rights and freedoms as a data subject, the data subject will be held responsible for any losses incurred as a result of such incorrect, incomplete, out-of-date, false, illegally acquired, or unauthorized use of personal data.

Section 2. Transmissibility of Rights of the Data Subject

In the event of the data subject's death or in the event that the data subject is unable to exercise the rights listed in the immediately preceding section, the data subject's legal heirs and assigns may make use of the rights to which they are entitled.

Section 3. Right to Data Portability

The data subject has the right to request a copy of his or her personal data from the PIC in an electronic or structured format that is frequently used and enables for further use by the data subject when it is processed using electronic means and in a structured and widely used format. The right of the data subject to control how his or her personal data is processed on the basis of consent or a contract, for business purposes, or by automated methods must be taken into consideration while exercising this right. The above-mentioned electronic format, as well as the technological standards, modalities, processes, and other guidelines for their transmission, may all be specified by the NPC.

Section 4. Limitation on Rights

If the processed personal data are used only for the purposes of scientific and statistical research and no actions are taken or decisions are made regarding the data subject as a result, the sections immediately preceding this one will not apply. However, the personal data must be held in strict confidence and used only for the stated purpose. Additionally, the aforementioned provisions do not apply to the processing of personal information obtained for the purpose of looking into a data subject's potential criminal, administrative, or tax responsibilities. Any restrictions placed on a data subject's rights must only go as far as is absolutely required to carry out the study or inquiry at hand.

Section 5. Inquiries and Complaints

Each data subject has the right to reasonable access to the personal information about them that the PIC or PIP is processing. Other rights include: (1) the right to contest the accuracy or error of the personal data; (2) the right to ask that the personal data be suspended, withdrawn, blocked, removed, or destroyed; and (3) the right to file a complaint and request compensation for any losses incurred as a result of inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of personal data.

Data subjects have the right to ask questions or make requests for information about any aspect of how their personal data is processed by the University, including the security and privacy measures used to safeguard such data. They may use official email to communicate with the university and provide a short explanation of the question as well as their contact information.

An official email address or three (3) printed copies of the complaint must be submitted. The responsible office must confirm the receipt of the complaint with the complainant.

PART 10. DATA BREACH NOTIFICATION

Section 1. Data Breach Notification

When the PIC or PIP learns of, or when there is a reasonable suspicion by the PIC or PIP that, a personal data breach requiring notification has occurred, it is required to notify the NPC and affected data subjects within seventy-two (72) hours.

When it is reasonable to believe that sensitive personal information or any other information that could, under the circumstances, be used to commit identity fraud has been obtained by an unauthorized person, and the PIC or the NPC believes that such unauthorized acquisition is likely to result in a real risk of serious harm to any affected data subject, notification of a personal data breach is required.

The NPC may look into the details of the personal data breach depending on the incident's severity, as well as any delays or failures to inform. Investigations could include checking out systems and processes in person.

Section 2. Contents of Notification

The notice must at the very least outline the kind of breach, any personal data that may have been compromised, and the steps the business has taken to remediate the breach. The notice must also contain any steps being taken to lessen the damage or unfavorable effects of the breach, the representatives of the PIC, along with their contact information, so that the affected data subjects may get more information about the breach.

Section 3. Delay of Notification

Only as long as is required to assess the severity of the breach, stop future disclosures, or restore the information and communications system's reasonable integrity may the notification be postponed. Page 27 of 29 in The CPSU Data Privacy Manual

The NPC may consider the PIC's compliance with this section and the presence of good faith in the collection of personal data when determining whether notification is needed.

If the NPC determines that notifying a PIC would not be in the best interests of the affected data subjects or the public, it may choose to do so.

If delaying notice might impede the development of a criminal investigation into a major violation, the NPC may approve delaying notification.

Section 4. Breach Report

The PIC must notify the NPC by providing a report—written or electronic—that includes all necessary notification information. The report must also provide the authorized PIC representative's name and contact information.

All security events and breaches of personal information, including those not subject to notification obligations, must be reported in writing. When there are personal data breaches, a report must include the circumstances of the occurrence, its consequences, and the corrective steps the PIC took. A report including aggregated data must be appropriate evidence for any other security events not affecting personal data. These reports must be made accessible upon NPC request. Each year, a broad overview of the reports must be sent to the NPC.

Section 5. Procedure for Notification

The DPA, its IRR, and any additional NPC issuances must all be followed in order for the breach notification procedure to be valid.

PART 11. OUTSOURCING AND SUBCONTRACTING AGREEMENTS

Section 1. Subcontract of Personal Data

In order to comply with the requirements of the DPA and its IRR, other applicable laws for the processing of personal data, and other issuances of the NPC, a PIC may subcontract or outsource the processing of personal data. However, in doing so, the PIC must use contractual or other reasonable means to ensure that adequate safeguards are in place, to ensure the confidentiality, integrity, and availability of the personal data processed, prevent its use for unauthorized purposes, and generally.

Section 2. Agreements for Outsourcing

A contract or other legal document that ties a PIP to the PIC must control processing done by that PIP.

The subject matter, length, nature, categories of data subjects, kind of personal data being processed, duties and rights of the PIC, and location of the processing in relation to the subcontracting arrangement must all be included in the contract or legal document.

The agreement or other legal document must specifically state that the PIP shall:

a. Process the personal data solely in accordance with the PIC's written instructions, including when transferring the data to another nation or an international organization unless the transfer is permitted by law;

b. Ensure that everybody with permission to treat the personal data is subject to a confidentiality duty;

c. implement suitable security measures, abide by the DPA, its IRR, and other NPC issuances;

d. not hire a different processor without the PIC's prior approval: Provided, however, that any such arrangement must guarantee that the same data protection responsibilities under the contract or legislative act are executed, taking into consideration the nature of the processing;

e. assist the PIC in fulfilling its commitment to respond to inquiries from data subjects about the exercise of their rights by using suitable technological and organizational methods and, to the degree practicable;

f. help the PIC, taking into consideration the kind of processing and the data at the PIP's disposal, ensure adherence to the DPA, its IRR, other relevant laws, and other NPC issuances;

g. After the completion of the services related to the processing, all personal data must be deleted or returned to the PIC at the PIC's discretion; provided, however, that existing copies must also be deleted unless storage is permitted under the DPA or another law;

h. Make all information required to prove compliance with the DPA's duties accessible to the PIC, and permit and assist with any audits or inspections carried out by the PIC or another auditor as directed by the latter.

i. If a directive, in the PIC's judgment, violates the DPA, its IRR, or any other directive issued by the NPC, the PIC must be notified right away.

Section 3. Duty of Personal Information Processor

In addition to the responsibilities stipulated in a contract or other legal act with a PIC, the PIP should abide by the requirements of the DPA and its IRR, other relevant laws, and other NPC issuances.

PART 12. RULES ON ACCOUNTABILITY

Section 1. Accountability for Transfer of Personal Data

A PIC is accountable for any personal data in its possession or under its control, including data that has been transferred to a PIP or another party for processing domestically or abroad, subject to cross-border agreements and co-operation.

A PIC is responsible for adhering to the DPA's and its IRR's criteria as well as those of other NPC issuances. To provide a similar degree of protection for the personal data when it is being processed by a PIP or third party, it must utilize contractual protections or other appropriate measures.

A PIC must name a person or people who will be responsible for ensuring that the DPA is followed. A data subject has the right to know the identity of the person or people specified in this way upon request.

Section 2. Accountability for Violations

Any individual—natural or legal—or other entity engaged in the processing of personal data that violates the DPA, its IRR, or other NPC directives is liable for the violation and is subject to the corresponding sanction, penalty, or fine. This is without prejudice to any potential civil or criminal liability.

When a data subject submits a complaint alleging that his or her rights as a data subject have been violated and that they have been harmed as a consequence of the processing of their personal data, the NPC may provide indemnification based on the relevant New Civil Code articles.

The individual who performed the illegal act or omission should be referred for prosecution by the NPC based on significant evidence in cases of criminal actions and their related personal punishment.

PART 13. Effectivity

The Board of Trustees' approval makes the contents of this Manual operative.

PART 14. Annexes