

UNIVERSITY OF THE PHILIPPINES SYSTEM
DATA PRIVACY MANUAL (2023 EDITION)

PART 1. INTRODUCTION.

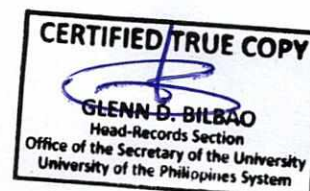
In order for the University of the Philippines (“UP” or “University”) to carry out its mandate under Republic Act No. 9500 (“RA 9500”, or the UP Charter) to exercise, among others, the right and responsibility of academic freedom guaranteed by the Constitution; to maintain and further develop its academic standards in the performance of its functions of instruction, research, extension, and public service; to enter into contracts in pursuance of its mandate and to comply with other legal obligations as a state university, including the duty to provide the public with information on matters of public concern as required by the Constitution, Republic Act No. 6713 (“RA 6713”), and its Implementing Rules and Regulations (“IRR”), it must necessarily collect, store, perform operations, retrieve or otherwise process the personal information of students, faculty, staff, officials, alumni, contractors, and other parties.

The University recognizes that it must adhere to the principles of transparency, legitimate purpose and proportionality in processing personal information, and to maintain such reasonable and appropriate physical, technical, and organizational measures in order to uphold the rights of data subjects and prevent the misuse of personal information that it processes.

The University, through its Board of Regents, adopts this Data Privacy Manual (“Manual”) pursuant to Republic Act No. 10173 (“RA 10173”), otherwise known as the Philippine Data Privacy Act of 2012 (“DPA”), its Implementing Rules and Regulations (IRR), and the applicable issuances of the National Privacy Commission (“NPC”), so as to enable the University to comply with the objective of the said DPA of protecting the fundamental human right of privacy of communication while ensuring the free flow of information in order to promote innovation and growth.

PART 2. SCOPE.

SECTION 1. This Manual shall apply to all University officials and personnel, such as faculty; research, extension, professional (“REPs”) and administrative staff; health service personnel; student assistants; and contractual personnel who process personal information pursuant to the instruction of the University as personal information controller (“PIC”) or



JUL 03 2023

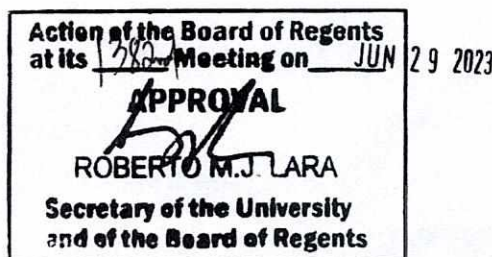
as personal information processor (“PIP”). Research, for example, is covered by this Manual only insofar as such research is undertaken or commissioned by the University, such that the processing of personal information is under the University’s control. This Manual likewise applies to contractors and service providers who act as PIPs of the University pursuant to the provisions of contracts between UP and such PIPs as required by the DPA. Offices and units of the Constituent Universities (“CUs”) as well as the Philippine General Hospital and Philippine Genome Center are required to adopt this Manual in order to comply with the minimum requirements of the DPA, its IRR and NPC issuances. In appropriate instances, CUs or their respective units, the Philippine General Hospital and Philippine Genome Center may propose and adopt a data privacy manual, subject to the approval by the Board of Regents, that provides for even more stringent standards when so warranted by the conditions in their respective campuses, including their access to personnel with specialised skill sets; funding and other resources; the complexity of their data processing operations; research obligations, issuances of the public authorities which apply to particular processing activities the nature of the personal data being processed, and other relevant considerations.

SECTION 2. Pursuant to the DPA, this Manual applies to personal information, regardless of the manner of storage. Filing systems covered by the DPA include those that are structured either by reference to individuals, or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

SECTION 3. The DPA and this Manual do not apply to the following:

(a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

- (1) The fact that the individual is or was an officer or employee of the government institution;
- (2) The title, business address and office telephone number of the individual;
- (3) The classification, salary range and responsibilities of the position held by the individual; and
- (4) The name of the individual on a document prepared by the individual in the course of employment with the government.



JUL 03 2023

(b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services.

(c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit.

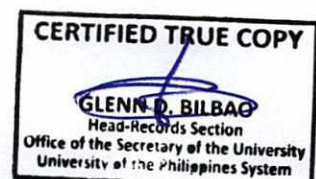
(d) Personal information processed for journalistic, artistic, literary or research purposes. For personal information processed for research purposes, in order to be exempt from the provisions of the DPA, the same must be intended for a public benefit and comply with applicable laws, rules and ethical guidelines. UP shall provide the necessary support in order to enable all its offices and units (e. g., the Philippine Genome Center) to establish research ethics committees or boards accredited by the Philippine Health Research Ethics Board at the soonest possible time, so that the necessary ethics clearance can be granted for research conducted by UP and its constituents.

(e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in the DPA shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the *Secrecy of Bank Deposits Act*; Republic Act No. 6426, otherwise known as the *Foreign Currency Deposit Act*; and Republic Act No. 9510, otherwise known as the *Credit Information System Act* (“CISA”).

(f) Information necessary for banks and other financial institutions under the jurisdiction of the independent central monetary authority, or *Bangko Sentral ng Pilipinas*, to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the *Anti-Money Laundering Act* and other applicable laws; and

(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

Provided, that the non-applicability of the DPA and this Manual does not extend to the University as a personal information controller (“PIC”) or personal information processor (“PIP”), and all persons processing information pursuant to the University’s instruction as PIC or PIP, who remain subject to the requirements of implementing security measures for



JUL 03 2023

personal data protection: *provided further*, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the DPA and this Manual only to the minimum extent necessary to achieve the specific purpose, function, or activity.

PART 3. DEFINITION OF TERMS.

SECTION 4. Whenever used in this Manual, the following terms shall have the respective meanings hereinafter set forth:

- (a) *Acceptable Use Policy* refers to a document or set of rules stipulating controls or restrictions that personnel of a PIC or PIP must agree to for access to the network, facilities, equipment, or services of such PIC or PIP.
- (b) *Access Control Policy* refers to a document or set of rules that defines how access to information is managed, including who may access specific information and under what circumstances.
- (c) *Automated Decision-making* refers to a wholly or partially automated processing operation that can make decisions using technological means totally independent of human intervention – automated decision-making often involves profiling.
- (d) *Business Continuity* refers to the capability of a PIC or PIP to continue the delivery of products or services at acceptable pre-defined levels following disruptive events.
- (e) *Business Continuity Plan* refers to documented procedures that guide PICs or PIPs to respond, recover, resume, and restore to a pre-defined level of operation following disruptive events.
- (f) *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 or 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.
- (g) *Control Framework* refers to a set of security measures that is a comprehensive enumeration of the organizational, physical, and technical measures intended to address risks, to the availability, integrity and confidentiality of personal data and to protect the personal data against natural dangers such as accidental loss, destruction, or contamination



JUL 03 2023

due to flood, fire and other similar events and human dangers such as unlawful access, fraudulent misuse, unlawful destruction and alteration.

(h) *Data Center* refers to a centralized repository, which may be physical or virtual, may be analog or digital, which may or may not be owned by the PIC or PIP used for the storage, management, and dissemination of data including personal data.

(i) *Data subject* refers to an individual whose personal information is processed.

(j) *Disruptive Events* refers to any occurrence or change that interrupts planned activities, operations, or functions, whether anticipated or unanticipated.

(k) *Encryption* refers to the reversible transformation of data by a cryptographic algorithm to produce ciphertext so as to hide the information content of the data.

(l) *Filing system* refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.

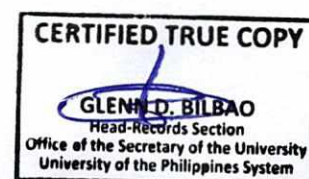
(m) *Government Agency* refers to a government branch, body, or entity, including national government agencies, bureaus, or offices, constitutional bodies, local government units, government-owned and controlled corporations, government financial institutions, state colleges and universities.

(n) *Information and Communications System* refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted or stored, and any procedure related to the recording, transmission or storage of electronic data, electronic messages, or electronic documents.

(o) *Off-The Shelf Software* refers to software product that is ready-made and commercially available for sale, lease, or licensed to the general public.

(p) *Password Policy* refers to a document or set of rules that passwords for a service must satisfy to increase the security and privacy of electronic devices.

(q) Other information that may be used to enable identity fraud shall include, but not be limited to, data about the financial or economic situation of the data subject; usernames; passwords and other login data; email addresses; biometric data; copies of identification



JUL 03 2023

documents, licenses or unique identifiers like PhilHealth, SSS, GSIS, TIN numbers; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

(r) *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.

(s) *Personal data* is the term used when referring to personal information, sensitive personal information, and privileged information collectively. For purposes of this Manual, and purely for UP's convenience, it may be used interchangeably with *personal information*, where appropriate.

(t) *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. A personal data breach may be in the nature of:

- (1) An availability breach resulting from loss, accidental or unlawful destruction of personal data;
- (2) Integrity breach resulting from alteration of personal data; and/or
- (3) A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.

(u) *Personal information controller* refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

- (1) A person or organization who performs such functions as instructed by another person or organization; and
- (2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

Action of the Board of Regents
at its 782nd Meeting on JUN 29 2023
APPROVAL

ROBERTO M. J. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

(v) *Personal information processor* refers to any natural or juridical person qualified to act as such under the DPA to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

(w) *Privacy Engineering* refers to the integration of privacy concerns into engineering practices for systems and software engineering life cycle processes.

(x) *Privacy-by-Design* is an approach to the development and implementation of projects, programs, and processes that integrates into the design or structure safeguards that are necessary to protect and promote privacy, such as appropriate organizational, technical, and physical policy measures.

(y) *Privacy-by-Default* is the principle according to which the PIC ensures that only data necessary for each specific purpose of the processing is processed by default (without the intervention of the user or the data subject).

(z) *Privacy Management Program* (“PMP”) is a holistic approach to privacy and data protection, important for all PICs and PIPs involved in the processing of personal data. It is intended to embed privacy and data protection in the strategic framework and daily operations of a PIC or its PIP.

(aa) *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.

(bb) *Privileged information* refers to any and all forms of data which, under the Rules of Court, other Supreme Court issuances, and pertinent laws, constitute privileged communication.

(cc) *Security Clearance* refers to permission granted to an individual to access information based on the given level of access.

(dd) *Security incident* is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It includes incidents that will result in a personal data breach, if not for safeguards that have been put in place;

(ee) *Sensitive personal information* refers to personal information:

Action of the Board of Regents
at its 382nd Meeting on JUN 29 2023
APPROVAL

ROBERTON M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

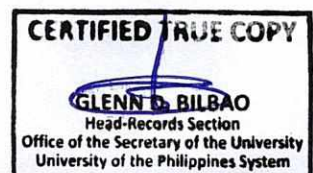
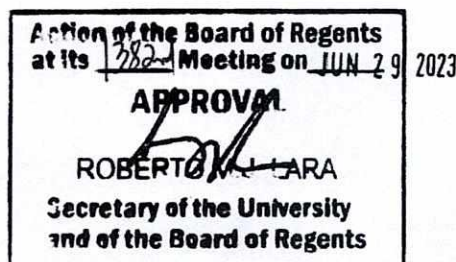
JUL 03 2023

- (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
 - (2) 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;
 - (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
 - (4) Specifically established by an executive order or an act of Congress to be kept classified.
- (ff) *System Management Tool* is a software system that facilitates the administration of user passwords and access rights.
- (gg) *Telecommuting* refers to work from an alternative workplace with the use of telecommunications or computer technologies (see Republic Act No. 11165, Section 3).
- (hh) *Vulnerable data subjects* include minors, the mentally ill, asylum seekers, the elderly, patients, those data subjects whose personal data involve criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a personal information controller or personal information processor (NPC Advisory Opinion 2018-077 and NPC Advisory Opinion 2021-043).

PART 4. DATA PRIVACY PRINCIPLES AND CRITERIA FOR LAWFUL PROCESSING.

SECTION 5. The University is cognizant of its obligation to adhere to the following general data privacy principles:

- (a) *Transparency.* The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of



JUL 03 2023

personal data should be easy to access and understand, using clear and plain language. UP's privacy notices are posted at <https://privacy.up.edu.ph/>

(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 data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

All persons who process personal information under the control of the University as PIC or PIP must see to it that personal information is:

(a) Collected for specified and legitimate purposes determined and declared before or, as soon as reasonably practicable, after collection and later processed in a way compatible with such declared, specified and legitimate purposes only;

(b) Processed fairly and lawfully;

(c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;

(d) Adequate and not excessive in relation to the purposes for which they are collected and processed;

(e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and

(f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: *provided*, that personal information collected for other purposes may be processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *provided further*, that adequate safeguards are guaranteed by said laws authorizing their processing.

SECTION 6. All persons who have been entrusted with processing personal information upon the instruction of the University acting as PIC or PIP must comply with Section 12 of the DPA which states that:

Action of the Board of Regents
at its 382nd Meeting on JUN 29 2023
APPROVAL

ROBERTO M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System
JUL 03 2023

The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

- (a) The data subject has given his or her consent;
- (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
- (d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
- (e) The processing is necessary in order to respond to a national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
- (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

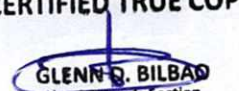
SECTION 7. All persons who process sensitive personal information and privileged information under the control of the University as PIC or PIP must see to it that Section 13 of the DPA, which provides the following, is complied with:

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

- (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
- (b) The processing of the same is provided for by existing laws and regulations: *provided*, that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *provided further*, that the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

Action of the Board of Regents
at its 782 Meeting on JUN 2 2023
APPROVAL

ROBERT M. TARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN B. BILBAD
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

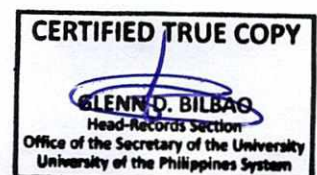
(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations; *provided*, that such processing is only confined and related to the bona fide members of these organizations or their associations; *provided further*, that the sensitive personal information are not transferred to third parties; *provided finally*, that consent of the data subject was obtained prior to processing;

(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

(f) The processing concerns such personal information as is 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.

SECTION 8. Under Section 15 of the DPA, the University as PIC may invoke the principle of privileged communication over privileged information that it lawfully controls or processes. Subject to existing laws and regulations, any evidence gathered from privileged information is inadmissible.

SECTION 9. The University recognizes that consent given by a data subject for the processing of his/her personal information or sensitive personal information may be withdrawn at any time. There are therefore limited instances in which processing by the University of personal and sensitive personal information will be based on consent. The vast majority of instances of processing flow from the University's mandate to exercise academic freedom in order to fulfill its obligation to uphold the right to quality education of students. Sensitive personal information, for example, in the form of educational records, birth dates, and other personal information are processed by the University in order to validate the identity of applicants and determine who are qualified to enroll in the University as UPCAT qualifiers, shiftees, transferees, graduate students, etc. Grades are processed in order to determine who are able to comply with the University's academic standards and who are qualified to graduate. Personal data of employees and contractual personnel, including their educational records for example, are also processed in order for the University to determine who are qualified to teach pursuant to its academic freedom.



JUL 03 2023

Other applicable laws and rules, e. g., GSIS, PhilHealth, Civil Service rules, BIR issuances, etc., also require UP to process the information of its personnel.

SECTION 10. UP personnel have the obligation to consult and seek guidance from relevant University offices, e. g., the proper DPO and legal office, in the event they are unsure of whether they are authorized to process or perform operations (access, copy use, disclose, etc.) on personal data. This obligation is contained in the non-disclosure undertaking (“NDU”) template of UP. See https://privacy.up.edu.ph/downloadable-forms/Memo_TJH2019-10_NDU-for-all-employees.pdf

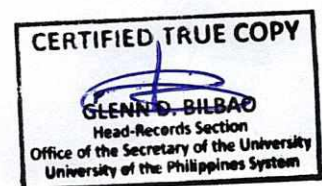
All persons to whom this Manual applies are reminded of the following criminal penalties under the DPA pertaining to unlawful or unauthorized processing of personal information:

“xxx

SEC. 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. – (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (PhP 500,000.00) but not more than Two million pesos (PhP 2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

(b) The unauthorized processing of sensitive personal information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (PhP 500,000.00) but not more than Four million pesos (PhP 4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

SEC. 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence. – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (PhP 500,000.00) but not more than Two million pesos (PhP 2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.



JUL 03 2023

(b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (PhP 500,000.00) but not more than Four million pesos (PhP 4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

xxx

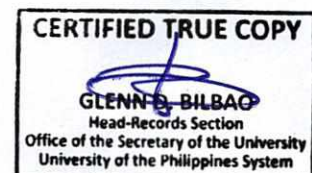
SEC. 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. – The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (PhP 500,000.00) but not more than One million pesos (PhP 1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (PhP 500,000.00) but not more than Two million pesos (PhP 2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

SEC. 29. Unauthorized Access or Intentional Breach. – The penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (PhP 500,000.00) but not more than Two million pesos (PhP 2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.

xxx

SEC. 31. Malicious Disclosure. – Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5)



JUL 03 2023

years and a fine of not less than Five hundred thousand pesos (PhP 500,000.00) but not more than One million pesos (PhP 1,000,000.00).

SEC. 32. *Unauthorized Disclosure.* – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (PhP 500,000.00) but not more than One million pesos (PhP 1,000,000.00).

(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (PhP 500,000.00) but not more than Two million pesos (PhP 2,000,000.00).

SEC. 33. *Combination or Series of Acts.* – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (PhP 1,000,000.00) but not more than Five million pesos (PhP 5,000,000.00).

xxx”

PART 5. ORGANIZATIONAL, PHYSICAL, AND TECHNICAL MEASURES


SECTION 11. The University, through the heads of offices and units, recognizes its responsibility to implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing. It shall 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.

SECTION 12. The University, through the heads of offices and units, is allowed under Section 20 of the DPA to take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and

UP SYSTEM DATA PRIVACY MANUAL 2023 EDITION

Action of the Board of Regents
at its 382nd Meeting on JUN 29 2023
APPROVAL

ROBERT M. LLARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

complexity of its operations, current data privacy best practices and the cost of security implementation, in determining what are reasonable and appropriate organizational, physical, and technical measures to be adopted, subject to such guidelines as may be issued by the NPC. The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines that the National Privacy Commission may issue from time to time, the measures implemented must include:

- (1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage, or interference with, or hindering of, their functioning or availability;
- (2) A security policy with respect to the processing of personal information;
- (3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and
- (4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

As stated below, UP must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

SECTION 13. Organizational Measures. The University, acting through the proper heads of offices and units, shall implement the following organizational measures as part of its Privacy Management Program (“PMP”):

(a) *Data Protection Officer (“DPO”) and Compliance Officer for Privacy (“COP”).* The University, through the UP President, shall appoint at least one Data Protection Officer (“DPO”) for each of the offices of the University System Administration, the Philippine General Hospital (“PGH”), and the Philippine Genome Center (“PGC”).

The UP President, in case of UP System Administration Offices, and, for the Constituent Universities, the Chancellors, may likewise appoint other DPOs for other UP offices or units. Such officials may also appoint compliance officers for privacy (COP), who may perform some of the functions of a data protection officer, pursuant to the issuances of the NPC, and upon the recommendation of, and subject to supervision by the proper DPO.

Action of the Board of Regents
 at its 1382 Meeting on JUN 29 2023
APPROVAL
 ROBERTO M. ARA
 Secretary of the University
 and of the Board of Regents

CERTIFIED TRUE COPY
 GLENN B. BILBAO
 Head-Records Section
 Office of the Secretary of the University
 University of the Philippines System

JUL 03 2023

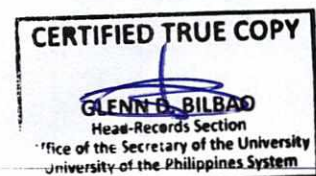
An individual researcher, *e. g.*, student, university research assistant (“URA”), or faculty, doing research commissioned or under the control of UP is automatically the COP for such research. If such research will be done by a group of researchers, at least one member of the research team must act as the COP.

DPOs and other compliance officers should be full-time, or organic employees of the University. Consultants and project, seasonal, probationary, or casual employees should not be designated as DPOs. The DPO should have expertise in relevant privacy or data protection policies and practices. He or she should have sufficient understanding of the processing operations being carried out by the University including the latter’s information systems, data security and/or data protection needs. The DPO shall have the appropriate rank, as provided under current NPC issuances, including Section 10 of NPC MC 2022-04. UP, through the proper officials, shall take such necessary steps so as to secure the proper plantilla items and budget from the Department of Budget and Management in order to be able to comply with the requirements of such NPC issuance. The UP President and Chancellors shall also see to it that the DPOs are provided with such human and other resources needed in order for them to efficiently and effectively carry out their functions.

The DPO shall have the following functions and responsibilities in relation to University offices, or, in the case of a researcher or research team, the research project, that are under their respective jurisdictions:

- (1) Monitor and assist the University with compliance with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies.
- (2) Assist University offices, units and personnel tasked with: (a) processing personal data in the conduct of a privacy impact assessment (“PIA”) relative to activities, measures, projects, programs, or systems of the University acting as PIC or PIP; (b) procurement and use of Off the Shelf Software; and, (c) in the case of research, also ensure that the protocol is reviewed by a research ethics board accredited by the Philippine Health Research Ethics Board before such research is conducted. See item 1 of Memo TJH 2019-07A at https://privacy.up.edu.ph/memos-and-issuances/MEMO_NO._TJH_2019-07A.PDF

The office or unit that processes personal data, and/or uses, or intends to procure and use Off the Shelf Software for its processing operations, has the obligation to inform the proper DPO of its existing, or proposed, data processing operations,



JUL 03 2023

including the existing or planned future use of Off the Shelf Software, to enable the DPO to help such office or unit conduct the PIA. UP shall ensure that general data privacy principles, and other data privacy and legal compliance requirements, are integrated into the design, up to the deployment of its data processing systems. Data privacy requirements that are identified must be enabled by default without requiring any action from the data subject.

(3) Advise the University regarding complaints and/or the exercise by data subjects of their rights or, in the case of research, the DPO of the research activity must act on such complaints or data subject requests.

(4) Provide assistance in the proper data breach and security incident management by the University or by the concerned researcher/s, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches through the NPC's electronic portal <https://dbnms.privacy.gov.ph/login> within the prescribed period with the assistance and timely submission by UP offices of the information needed for such reports and documentation.

(5) Inform and cultivate awareness on privacy and data protection including all laws, rules regulations and issuances within the University or in the case of research within the research team, as well as all those who will process research data, *e. g.*, research assistants, transcribers, and other third party providers.

(6) Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the University relating to privacy and data protection, by adopting a privacy by design approach.

(7) Serve as the contact person of the University *vis-à-vis* data subjects, the NPC and other authorities in all matters concerning data privacy, or security issues or concerns.

(8) Cooperate, coordinate and seek the advice of the NPC regarding matters concerning data privacy and security; and

(9) Perform other duties and tasks that may be assigned by the University that will further the interest of data privacy and security, and uphold the rights of the data subjects; *provided*, that such additional duties must not involve a conflict of interest. *Conflict of interest* refers to a scenario wherein a DPO is charged with performing tasks, duties, and responsibilities that may be opposed to or could affect

Action of the Board of Regents
at its ~~782~~ Meeting on JUN 28 2023
APPROVAL
ROBERTO M. ARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY
GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

his or her performance as DPO. This includes, *inter alia*, holding a position within the University that leads him or her to determine the purposes and the means of the processing of personal data.

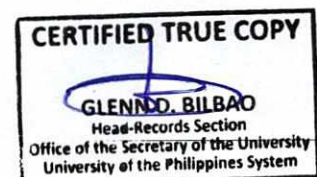
In addition to the above functions, the UP System Data Protection Officer shall provide System-wide coordination of UP's data privacy compliance activities by:

- (1) providing guidance and assistance to the other UP DPOs and COPs whenever appropriate and necessary as in the case especially of newly appointed DPOs and COPs; and
- (2) proposing System-wide policies, programs of action, privacy notices, template PIA and other data privacy compliance forms, subject to democratic consultation with the proper UP System administration, and CU officials, offices and units; and
- (3) issuing Systemwide or UP System Administration privacy notices, template PIA and other data privacy compliance forms, subject to democratic consultation with the proper UP System administration, and when applicable, CU or other unit officials, offices and units.

To enable the UP System DPO to effectively perform such functions, and to see to it that the registration information submitted by DPOs to the NPC for the same data processing system used by the UP System administration and CU units and offices is uniform and consistent, the UP President, or his or her duly authorized representative, shall periodically require all UP offices and units throughout the UP System (which includes offices or units of the CUs and/or their DPOs) to submit to the UP System DPO a copy of relevant PIAs for their data processing systems.

(b) *Records of Processing Activities.* University offices, as well as researchers conducting research commissioned by or under the control of UP, shall maintain records that sufficiently describe their respective data processing systems, and identify the duties and responsibilities of those individuals who will have access to personal data. Such offices and researchers must provide DPOs with such records in order to enable UP to register such systems and assist these offices and researchers to conduct the proper PIAs. Such records should include (per data processing system):

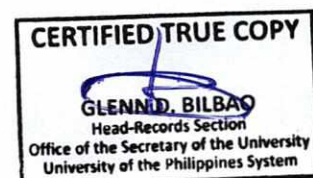
- (1) name of the data processing system;



JUL 03 2023

- (2) basis or bases for the processing of information;
- (3) purpose or purposes of the processing;
- (4) whether processing is being performed as a PIC or PIP, if an organization uses the same system as a PIC and as a PIP, then the organization shall register such usage separately;
- (5) whether the system is outsourced or subcontracted, and if so, the name and contact details of the PIP;
- (6) description of the category or categories of data subjects, and their personal data or categories thereof;
- (7) recipients or categories of recipients to whom the personal data might be disclosed;
- (8) description of security measures (Organizational, Physical, and Technical);
- (9) general information on the Data Life Cycle (Time, Manner, or Mode of Collection, Retention Period, and Disposal/Destruction/Deletion Method/Procedure);
- (10) whether personal data is transferred outside of the Philippines;
- (11) the existence of Data Sharing Agreements with other parties;
- (12) whether the data processing system is a publicly facing online mobile or web-based application, including internal apps with PIC or PIP employees as clients; and
- (13) whether the system makes use of wholly or partly automated decision-making operation or profiling.

(c) *Privacy Impact Assessment.* The University shall ensure that privacy impact assessments conducted by its offices, data protection and compliance officers, as well as researchers, are proportionate or consistent with the size and sensitivity of the personal data being processed, and the risk of harm from the unauthorized processing of that data. All officials, personnel and offices are required to provide complete and accurate information to DPOs and compliance officers for privacy (“COPs”) that assist offices and units in conducting PIAs. In order to comply with the privacy by design approach, offices and units must, with the assistance of the proper DPO, conduct a PIA within a reasonable time



before processing operations are commenced, especially those which involve sensitive personal information and information which may be used to perpetrate identity fraud, as well as those which involve public facing Internet and/or applications (“app”) based portals.

The following shall be taken into account when conducting a PIA: (1) confidentiality breach; (2) integrity breach; (3) availability breach; (4) infringement of the general data privacy principles; and (5) violations of rights of data subjects.

The PIA shall include the following:

- (1) a data inventory identifying:
 - (i) the types of personal data held by the University office or unit, including records of its own personnel;
 - (ii) list of all information repositories holding personal data, including their location;
 - (iii) types of media used for storing the personal data; and
 - (iv) risks associated with the processing of the personal data;
- (2) a systematic description of the personal data to be, or that is being, processed, the purposes for such processing (including anticipated purposes), as well as the lawful basis or bases for such processing (including anticipated processing operations), and the purposes of the processing;
- (3) an assessment of the necessity and proportionality of the processing in relation to the purposes of the processing;
- (4) a holistic assessment of the risks to the rights and freedoms of a data subject;
- (5) an assessment of risks to the confidentiality, integrity and availability of personal data; and
- (6) an assessment of physical, organizational and technical measures to address identified risks.

Such assessment shall be updated as necessary (*e. g.*, new features or major changes in processing, new regulations, new contract entered by the PIC or change in service provider or PIP). Likewise, control frameworks that were previously assessed, and



implemented shall be monitored, evaluated, updated accordingly, and incorporated as a component of a PIC's PMP.

The risks identified in the PIA must be addressed by a control framework. The contents of a control framework shall take into account, among others, the following: (1) nature of the personal data to be protected; (2) risks represented by the processing, the size of the organization, and the volume of its operations; (3) current data privacy best practices in a specific industry; (4) cost of security implementation; and (4) purpose and extent of data sharing or outsourcing agreements and their attendant risks.


(d) *Management of Human Resources.* The University shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data. All employees, personnel, agents, or representatives with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure. This obligation shall continue even after leaving the public service, transferring to another position, or upon terminating their employment or contractual relations. There shall be capacity building, orientation or training programs for such employees, agents or representatives, regarding privacy or security policies as often as may be necessary. Heads of offices and units shall see to it that such personnel, agents or representatives attend data privacy training activities. Such officials shall likewise ensure that personnel as well as third persons processing personal data for their offices execute and submit the proper non-disclosure undertaking ("NDU") in favor of the University as required by Memorandum TJH 2019-10. https://privacy.up.edu.ph/downloadable-forms/Memo_TJH2019-10_NDU-for-all-employees.pdf

(e) *Security Clearance for Processing Sensitive Personal Information.*

(1) *On Site and Through On-Line Access Under Section 23 of the DPA.* The University shall strictly regulate access to sensitive personal data under its control or custody, and shall grant to agency personnel a security clearance to access the same on government property, or through online facilities, only when the performance of official functions or the provision of a public service directly depends on such access, or cannot otherwise be performed unless such access is allowed to such agency personnel. All security clearances shall be issued by the head of the source agency. The source agency is the University office that originally collected the personal data. A copy of each security clearance must be filed with the proper Data Protection Officer.

Action of the Board of Regents
at Its 582nd Meeting on JUN 29 2023
APPROVAL

ROBERTO M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN B. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

(2) *Off-site Access Under Section 23 of the DPA.* Unless otherwise provided in guidelines to be issued by the NPC, sensitive personal information maintained by an agency may not be transported or accessed from a location off government property unless a request for such transportation or access is submitted and approved by the head of the source agency in accordance with the following guidelines:

(i) *Deadline for Approval or Disapproval.* In the case of any request submitted to the head of the source agency, such head of the source agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;

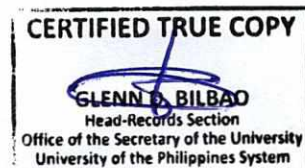
(ii) *Limitation to One thousand (1,000) Records.* If a request is approved, the head of the source agency shall limit the access to not more than one thousand (1,000) records at a time; and

(iii) *Encryption.* Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard recognized by the National Privacy Commission ("NPC").

(f) *Contracts with Personal Information Processors ("PIP").* The University, through appropriate contractual or other legal acts, shall ensure that its PIPs, where applicable, shall also comply with the DPA, its IRR and the issuances of the NPC, including the provisions for implementing security measures.

Processing by a PIP shall be governed by a contract or other legal act that binds the PIP to the University. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the PIC, and the geographic location of the processing under the subcontracting agreement. The UP office or unit primarily responsible for procuring and/or availing of the services of such PIP shall see to it that the contract or other legal act shall stipulate, at the minimum, and in particular, that the PIP shall:

(1) Process the personal data only upon the documented instructions of the University, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;

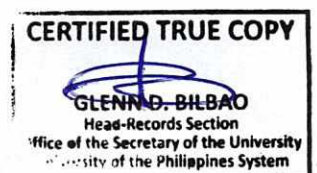


JUL 03 2023

- (2) Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data;
- (3) Implement appropriate security measures and comply with the DPA and its IRR, and other issuances of the NPC;
- (4) Not engage another processor without prior instruction from the University; *provided*, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;
- (5) Assist the University, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;
- (6) Assist the University in ensuring compliance with the DPA and its IRR, other relevant laws, and other issuances of the NPC, taking into account the nature of processing and the information available to the PIP;
- (7) At the choice of the University, delete or return all personal data to the University after the end of the provision of services relating to the processing; *provided*, that this includes deleting existing copies, unless storage is authorized by the DPA or another law;
- (8) Make available to the University all information necessary to demonstrate compliance with the obligations laid down in the DPA, and allow for and contribute to audits, including inspections, conducted by the PIC or another auditor mandated by the latter; and
- (9) Immediately inform the University if, in its opinion, an instruction infringes the DPA and its IRR, or any other issuance of the NPC.

Notwithstanding the foregoing, UP may impose additional obligations upon the PIP when such will help uphold the rights of data subjects.

The office or unit primarily responsible for procuring and/or availing of the services of such PIP shall ensure that the required provisions for DPA compliance set forth above are included in the contract or addendum to such contract, and must submit a copy of the contract or legal act containing the abovementioned provisions to the proper DPO. See TJH 2020-21 for the data privacy compliance template for PIPs <https://privacy.up.edu.ph/memos-and->



JUL 03 2023

issuances/MEMORANDUM%20NO.%20TJH%202020-21%20DATA%20PRIVACY%20COMPLIANCE%20PROVISIONS%20FOR%20CONTRACTS%20OR%20AGREEMENTS%20BETWEEN%20UP%20AND%20PERSONAL%20INFORMATION%20PROCESSORS%20(PIPS).pdf

(g) *Creation and Continuing Review of Relevant Policies.* The University shall continue to enforce the *Acceptable Use Policy Policy for Information Technology Resources of the UP System* (“AUP”). See <https://up.edu.ph/approved-acceptable-use-policy-for-information-technology-it-resources-of-the-up-system/>

It shall create privacy and data protection policies to set and standardize the governance of the processing of personal data, taking into account the results of the privacy impact assessments, as well as Sections 25 to 29 of the IRR of the DPA. Privacy and security policies and practices within the University shall be periodically reviewed and updated in order to ensure that the same are consistent with current data privacy best practices in the industry as well as applicable laws and issuances. The University shall comply with NPC’s orders when its privacy and data protection policies are subject for review and assessment in terms of their compliance with the requirements of the DPA, its IRR and all relevant issuances of the NPC.

(h) *Privacy Engineering.* As stated above, the University shall adopt Privacy-by-Design principles in developing, implementing, and deploying systems, processes, software, hardware, and services throughout the processing of personal data.

The University shall see to it that functions that do not have legal basis for processing or are incompatible with the specific, declared, and intended purposes of processing are switched off or deactivated.

If the University develops or implements a data processing system or software application that carries out any automated processing operations it shall embed Privacy-by-Design and Privacy-by-Default principles as well as data protection measures throughout the automated processing.

If the University carries out any wholly or partly automated processing operations, or set of such operations, intended to serve a single purpose, or several related purposes, it shall notify the NPC pursuant to existing issuances regarding any automated decision-making operation, or profiling, used to make decisions about a data subject.

A. The notification shall include the following information:

- (1) Purpose of processing;

Action of the Board of Regents at its 382nd Meeting on JUN 29 2023
APPROVAL
ROBERTO M. LARA
Secretary of the University and of the Board of Regents

CERTIFIED TRUE COPY
GLENN B. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

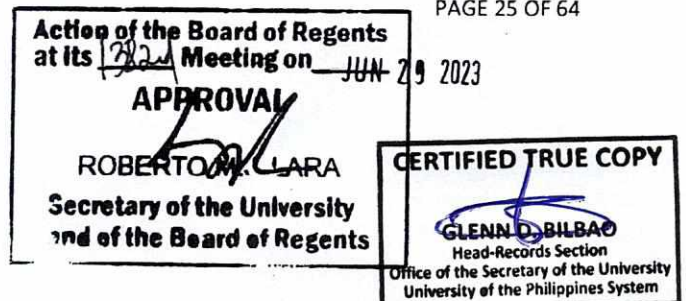
- (2) Categories of personal data to undergo processing;
- (3) Category or categories of data subject;
- (4) Consent forms or manner of obtaining consent when consent is the applicable basis for processing;
- (5) The recipients or categories of recipients to whom the data are to be disclosed;
- (6) The length of time the data are to be stored;
- (7) Methods and logic utilized for automated processing;
- (8) Decisions relating to the data subject that would be made on the basis of processed data or that would significantly affect the rights and freedoms of a data subject; and
- (9) Names and contact details of the Compliance or Data Protection Officer.

B. No decision with legal effects concerning a data subject shall be made solely on the basis of automated processing without the consent of the data subject, unless there is another lawful basis for such processing other than consent.

(i) *Data Privacy Training*. UP shall conduct PIC-wide training, as applicable, on privacy and data protection policies at least once a year, and as may be deemed necessary by the University; *provided*, that there shall also be a similar training conducted during all orientations for newly hired or contracted personnel or organizations by the University.

(j) *Business Continuity Plan* ("BCP"). The University shall continue to further develop its business continuity plan to mitigate potential and foreseeable disruptive events. It must consider the following:

- (i) Personal data backup, restoration and remedial time;
- (ii) Periodic review and testing of the business continuity plan which takes into account disaster recovery, privacy, a business impact assessment, a crisis communications plan, and a telecommuting policy, among others; and
- (iii) Contact information and other business-critical matters (*i. e.*, electrical supply, building facilities, IT assets).



JUL 03 2023

UP shall communicate its telecommuting policy and provide means to enable its personnel to securely telecommute, subject to applicable laws, rules and regulations. It must consider providing the following:

- (i) Training on the acceptable use of company-issued computing devices;
- (ii) Password management and secure practices in online accounts, computers, mobile phones and network appliances;
- (iii) Secure configuration of office-issued computers; and
- (iv) Periodic trainings on data privacy, cyber security, and online productivity, among others.

The current *Work From Home Advisory* is available at <https://privacy.up.edu.ph/advisories/ADVISORY%20ON%20DATA%20PRIVACY%20WHILE%20ON%20WORK.pdf>

SECTION 14. *Physical Security Measures.* The heads of offices and units shall see to it that the following physical security measures are complied with in their respective offices or units:

(a) *Access to Data Centers.* Personal data being processed by the University shall be stored in data centers, which may or may not be owned by the University. A data center is a centralized repository, which may be physical or virtual, may be analog or digital, used for the storage, management, and dissemination of data, including personal data. The same should be located away from general office space as well as areas that are accessible to the public; *provided*, that where a PIP is engaged for such data center, the NPC may require the University to submit its contract with its PIP for review.

Access to all data centers owned by the University should be restricted to personnel that have the appropriate clearance. This should be enforced by an access control system that records when, where, and by whom said data centers are accessed. Access records and procedures shall be reviewed by the University regularly. If personal data is stored in paper files or any physical media, the University office concerned shall maintain a log from which it can be ascertained which file was accessed, including when, where, and by whom. Such log shall also indicate whether copies of the file were made. Administration shall regularly review the log records, including all applicable procedures.

(b) *Access and Design of Workstations.* Access to workstations where personal data are being processed shall be restricted to personnel who are authorized to process such data.



JUL 03 2023

Such workstations should be located and designed so as to enable personnel to safeguard the confidentiality of such data. There should, for instance, be adequate space or distance between computer terminals.

(c) *Secure Location of Data Centers and Workstations.* Data centers and workstations where personal data are processed must, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

(d) *Measures When Computer or Paper Files Are Not Being Used.* Personnel shall see to it that they log out of the University's information and communications technology ("ICT") based data processing systems, and that their screens are locked whenever they leave computers unattended. Papers or documents containing personal information as well as portable storage devices, such as USBs, shall be encrypted as mentioned below and, where practicable, secured through a passkey and kept in locked cabinets when not being used. Printouts of documents kept in electronic form should not be left in areas where unauthorized persons may access them, such as in printers. When such printouts are no longer needed, the same must be securely disposed of through shredding.

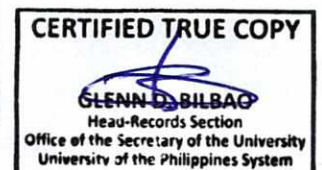
SECTION 15. Technical Security Measures. The University shall continue to enforce and implement the technical measures provided under the *Acceptable Use Policy for Information Technology Resources of the UP System* ("AUP"), pending approval by the Board of Regents of the *UP System Information Technology Security Policy*. UP shall endeavor to comply with the following technical measures contained in applicable NPC issuances:

(a) All personal data that are processed must be adequately protected through industry standards and best practices.

(b) Passwords or passphrases used to access personal data should be of sufficient strength to deter password attacks. A password policy should be issued and enforced through a system management tool.

(c) Personnel who access sensitive personal information, privileged information, and a high volume of personal data online shall authenticate their identity via a secure encrypted link and must use at least a multi-factor authentication (*e. g.*, one-time pin ["OTP"], security code). Such access rights must be defined and controlled by a System Management Tool.

(d) Only programs licensed or owned, or individuals authorized, by the PIC shall be allowed to access or modify databases containing the personal data under its control.



JUL 03 2023

(e) Generally, local copies of personal data may not be accessed, processed or stored on local machines without appropriate security control measures and protection that prevents unauthorized access. A PIC or PIP may adopt and utilize technologies that prevent personal data, accessible online to authorized personnel, from being copied to a local machine, or the computer that a user is currently using on a computer network. Where possible, a PIC or PIP personnel shall not be allowed to save files to a local machine and to instead save files to their allocated network drive. Drives and USB ports on local machines may also be disabled as a security measure. A PIC or PIP may also consider prohibiting the use of cameras in areas where personal data is visible or processed. A PIC or PIP may likewise provide technologies for the automatic deletion of temporary files that may be stored on a local machine by its operating system.

(f) The University shall adopt reasonable and appropriate security measures to ensure that only authorized users are able to access the personal data processed by UP.

The University may also put in place solutions, which only allow authorized media to be used on its computer equipment.

(g) The University may adopt and use technologies that allow the remote disconnection of a mobile device owned by UP which has access to UP's data, or the deletion of personal data contained therein, in the event such mobile device is lost. It is the duty of University personnel to whom such mobile devices have been issued for official use to immediately report its loss to the head of unit and the proper Chancellor, or to the UP President, relevant DPO, and the UP System DPO, in order to enable UP offices to remotely disconnect and/or delete personal data and other confidential information, as well as other reasonable and appropriate measures to deal with the risks associated with such loss.


(h) In the event the University and or its personnel transfer data by email it must ensure that the data is adequately protected and use secure transmission and reception of email messages, including their attachments. Refer to https://privacy.up.edu.ph/instructions-and-guides/Encrypting_Files_prior_to_sharing.html

(i) University personnel who are authorized to copy personal data to personal productivity software in order to perform their duties or functions shall be reminded to securely process the same by, for example, locking their devices when not in use, using a password for securing files and other similar means.

(j) The use of optical media such as compact discs, digital versatile discs, and USB flash drives for processing personal data, shall be regulated; *provided*, that if such mode of

Action of the Board of Regents
at its 382nd Meeting on JUN 29 2023
APPROVAL

ROBERTON L. LARA
Secretary of the University
Member of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

transfer is unavoidable or necessary, then encryption shall be implemented in the removable or portable storage media.

(k) Where possible, the manual transfer of personal data, such as through the use of removable physical media like compact discs, shall not be allowed; *provided*, that if such mode of transfer is unavoidable or necessary, authentication technology, such as one-time PINs, shall be implemented.

(l) Facsimile technology shall not be used for transmitting documents containing personal data.

(m) When the University transmits documents or media containing personal data by mail or post, it shall make use of registered mail or, where appropriate, guaranteed parcel post service. It shall establish procedures that ensure that such documents or media are delivered only to the person to whom they are addressed, or his or her authorized representative; *provided*, that similar safeguards shall be adopted relative to documents or media transmitted between offices or personnel within the agency. Said documents or media shall be placed inside sealed envelopes.

(n) The University shall comply with its obligations under Republic Act No. 9470 ("RA 9470"), otherwise known as the *National Archives of the Philippines Act of 2007*.

See <https://www.officialgazette.gov.ph/2007/05/21/republic-act-no-9470/> and its IRR https://osu.up.edu.ph/wp-content/uploads/2016/03/10-Annexes_04.pdf

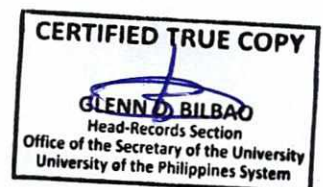
(o) In establishing policies and procedures for disposal of personal data, UP shall take into consideration the following:

- (i) Set retention period of data;
- (ii) Jurisdiction-specific laws, regulations, and existing contracts;
- (iii) Identify relevant de-identification, anonymization, or deletion techniques for specific types of data;
- (iv) Required documentation before the deletion, de-identification, or anonymization of personal information.

(p) In order to prevent the unauthorized disclosure of personal information, the University shall require the shredding of documents containing such information and provide for the secure disposal of computer equipment, such as disk servers, desktop computers, and mobile phones at end-of-life, especially storage media; *provided*, that the procedure shall

UP SYSTEM DATA PRIVACY MANUAL 2023 EDITION

PAGE 29 OF 64



JUL 03 2023

include the use of degaussers, erasers, and physical destruction devices, and disposal of personal data stored offsite.

Refer to the following data privacy compliance memoranda issued pursuant to the authority of the UP President:

https://privacy.up.edu.ph/memos-and-issuances/MEMO_NO._TJH_2019-07A.PDF

[https://privacy.up.edu.ph/memos-and-issuances/\[MEMO%20TJH%202021-10\]%20Reminder%20that%20faculty%20and%20students%20must%20use%20UP%20Mail%20for%20official%20correspondence%20and%20data%20privacy%20and%20security%20measures%20required%20for%20sending%20attachments%20and%20sharing%20G.pdf](https://privacy.up.edu.ph/memos-and-issuances/[MEMO%20TJH%202021-10]%20Reminder%20that%20faculty%20and%20students%20must%20use%20UP%20Mail%20for%20official%20correspondence%20and%20data%20privacy%20and%20security%20measures%20required%20for%20sending%20attachments%20and%20sharing%20G.pdf)

[https://privacy.up.edu.ph/memos-and-issuances/\[MEMO%20TJH%202021-11\]%20Reminder%20that%20classes%20and%20class%20related%20activities%20must%20be%20conducted%20using%20UPs%20learning%20.pdf](https://privacy.up.edu.ph/memos-and-issuances/[MEMO%20TJH%202021-11]%20Reminder%20that%20classes%20and%20class%20related%20activities%20must%20be%20conducted%20using%20UPs%20learning%20.pdf)

Personnel must likewise comply with the *Work From Home Advisory*
<https://privacy.up.edu.ph/advisories/ADVISORY%20ON%20DATA%20PRIVACY%20WHILE%20ON%20WORK.pdf>

All persons to whom this manual applies are reminded that under Section 27 of the DPA:

(a) The improper disposal of personal information shall be penalized by imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (PhP 100,000.00) but not more than Five hundred thousand pesos (PhP 500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

(b) The improper disposal of sensitive personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (PhP 100,000.00) but not more than One million pesos (PhP 1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

Action of the Board of Regents
at its 12th Meeting on JUN 29 2023
APPROVAL
[Signature]
ROBERTO M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY
[Signature]
GLENN B. BILBAO
Head-Records Section
Office of the Secretary of the University
of the Philippines System

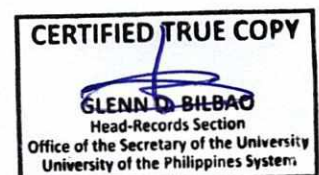
JUL 03 2023

PART 6. RIGHTS OF THE DATA SUBJECT.

SECTION 16. The University recognizes that a data subject, as well as his/her heirs or assigns, in the case of the former's death or incapacity, have the right to:

- (a) be informed whether personal information pertaining to him or her shall be, are being or have been processed;
- (b) be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:
 - (1) Description of the personal information to be entered into the system;
 - (2) Purposes for which they are being or are to be processed;
 - (3) Scope and method of the personal information processing;
 - (4) The recipients or classes of recipients to whom they are or may be disclosed;
 - (5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
 - (6) The identity and contact details of the personal information controller or its representative;
 - (7) The period for which the information will be stored; and
 - (8) The existence of their rights, *i. e.*, to access, correction, as well as the right to lodge a complaint before the NPC.

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification to the data subject; *provided*, that the notification under subsection (b) shall not apply should the personal information be needed pursuant to a *subpoena*, or when the collection and processing are for obvious purposes, including when it is necessary for the performance of, or in relation to, a contract or service, or when necessary or desirable, in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of a legal obligation.



JUL 03 2023

- (c) reasonable access to, upon demand, information regarding the processing of his/her personal information;
- (d) dispute the inaccuracy or error in the personal data and request its correction, unless such request is vexatious or unreasonable;
- (e) request the suspension, withdrawal, blocking, removal or destruction of personal data from the personal information controller's filing system upon discovery and substantial proof that the personal information is incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes, or are no longer necessary for the purposes for which they were collected;
- (f) complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data; and
- (g) the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The NPC may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer.

The abovementioned rights are not applicable if the processed personal information is used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject; *provided*, that the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the abovementioned rights are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.

SECTION 17. In order for the University to keep personal information accurate, data subjects, such as students and University personnel, must also provide correct information and update the concerned University offices if there are changes at the soonest possible time. In some cases, these can be done by the data subjects concerned through online processes using the University's applicable information systems.

SECTION 18. A data subject may request information relating to the processing of his/her personal information, its correction, or removal from UP's data processing system by submitting the proper form prescribed by UP offices in person, via post, or by email to the proper University office having jurisdiction over the request. In lieu of such form, the

Action of the Board of Regents
at its 1382nd Meeting on JUN 29 2023
APPROVAL

ROBERTO M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAG
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

requesting party may send a letter or email containing sufficient information to enable UP to process such request. Because of the complexity of UPs processing operations, it is necessary for the data subject, among others, to identify the specific data processing operation or system to which the request pertains, *e. g.*, UPCAT Online, SFA Online. There are requests that are governed by specific University policies, procedures and/or application forms that shall apply instead of the provisions in this section on the right of data subjects, such as the correction of grades, issuance of true copy of grades, transcript of records, etc.

The requesting party must likewise provide relevant documents in order to support his or her request, as well as a copy of his or her UP ID, or government issued ID ("GIID") card (*e. g.*, Phil ID or national ID under the *Philippine Identification System Act*), and if the application is made by a data subject's authorized representative, the authorization letter and the abovementioned identification cards of the data subject and his or her representative. If the request is made by an heir, s/he must provide UP with the relevant death certificate, marriage and or birth certificate, and other relevant supporting documents, as well as his or her GIID.

SECTION 19. The relevant office shall act on the request of the data subject mentioned in Section 18 above pursuant to the applicable provisions of Republic Act No. 11032 ("RA 11032") and NPC Advisory No. 2021-01 (dated 29 January 2021) and other laws, rules and issuances.

SECTION 20. The responsible staff of the relevant office shall check the completeness of the application, relevant supporting documents, if any, and the abovementioned identification cards or documents used for verifying the identity of the requesting party, or that of his/her authorized representative or heir.

The responsible office staff shall acknowledge receipt of the request if the application, supporting documents, and identification documents are complete and indicate the date when the same shall be acted on by the office if it has jurisdiction over the request. If the application is incomplete the staff shall inform the applicant of the deficiency of such application and identify or enumerate all the missing requirements. The period for processing such application shall start only from the time all the requirements for the application are submitted to the proper office. If the request is not within the jurisdiction of said office, the same shall be referred to the proper office and a copy of such referral shall be given to the requesting party. The period for processing the request shall run from the time the referral was received by the proper office.



JUL 03 2023

SECTION 21. All complete applications or requests submitted shall be acted upon by the assigned officer or staff within the prescribed processing time, which shall not be longer than the following periods counted from the date the complete application or request was received:

- (1) three (3) working days in the case of applications or requests submitted by applicants or requesting parties of a government office or agency which only require ministerial actions on the part of the public officer or employee, or that which present only inconsequential issues for the resolution by an officer or employee of said government (simple transactions);
- (2) seven (7) working days in the case of applications or requests submitted by applicants or requesting parties of a government office which necessitate evaluation in the resolution of complicated issues by an officer or employee of said government office, such transactions to be determined by the office concerned (complex transactions);
- (3) twenty (20) working days or as determined by the government agency or instrumentality concerned, whichever is shorter, for applications or requests involving activities which pose a danger to public health, public safety, public morals, public policy, and highly technical applications.

The maximum time prescribed above may be extended only once for the same. Prior to the lapse of the processing time, the office or agency concerned shall notify the applicant or requesting party in writing of the reason for the extension and final date of release of the government service/s requested. Such written notification shall be signed by the applicant or requesting party to serve as proof of notice.

In cases where the cause of delay is due to force majeure or natural or man-made disasters, which result in damage or destruction of documents, and/or system failure of the computerized or automatic processing, the prescribed processing times stated above shall be suspended and appropriate adjustments shall be made.

No application or request shall be returned to the applicant or requesting party without appropriate action. In case an application or request is disapproved, the officer or employee who rendered the decision shall send a formal notice to the applicant or requesting party within the prescribed processing time, stating therein the reason for the disapproval.

Action of the Board of Regents
at its 282nd Meeting on JUN 29 2023
APPROVAL
[Signature]
ROBERTO M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY
[Signature]
GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023


SECTION 22. A data subject may lodge a written complaint with the relevant DPO, via the DPO's official email, regarding how his/her personal information is being, or has been, processed, how a request for correction, deletion, etc., under Section 17 has been handled, or for other possible violations of the DPA or this Manual relating to the processing of his/her personal information. The data subject must state his/her name, contact details and narrate all relevant facts relating to the complaint. The complainant must likewise provide a copy of his/her UP ID or government issued ID (e. g., Phil ID or national ID under the *Philippine Identification System Act*) for verification purposes. The DPO shall acknowledge receipt of the complaint within three (3) working days. The DPO shall have the authority to require the complainant to provide additional information or documents when necessary, verify the allegations contained in the complaint, conduct an inquiry, and perform such other acts that are necessary in order to recommend action(s) to the proper Chancellor or the UP President. If the complaint involves a security incident or personal data breach the provisions of Part 7 below will apply, and the DPO will refer the matter to the proper officials. The DPO shall endeavor to provide his/her recommendation within thirty (30) working days from acknowledgment of receipt of the complaint. If a longer period is needed, the DPO will provide an update to the data subject describing what is being done regarding the complaint. As the DPO is only authorized to provide advice to the University under NPC advisory 2017-01 (dated 14 March 2017), it is the Office of the Chancellor or UP President that shall render a decision regarding the data subject's complaint. A motion for reconsideration of the decision of the Chancellor or the UP President may be filed by any affected party within fifteen days after receipt of the decision. If no such motion is filed within such period, the decision of the Chancellor or the UP President will become final and executory.

PART 7. SECURITY INCIDENT OR BREACH RESPONSE PROCEDURES.

SECTION 23. The University shall continue to enforce the provisions of the *Acceptable Use Policy for Information Technology Resources of the UP System* ("AUP") regarding the reporting mechanism and investigation of violations that constitute security incidents or data breaches. Per the AUP, it is the duty of every member of the University community to immediately inform the head of unit whose data processing system may have been (or has been) breached, or is the subject of a security incident, and the Office of the UP President, and/or the Chancellor, as well as the UP System DPO and proper DPO, of such possible or confirmed security incident or personal data breach. In the case of incidents or breaches involving ICT systems that process personal information, the head of the IT office acting as network or system administrator of the affected system shall likewise be

Action of the Board of Regents
at its 282nd Meeting on JUN 29 2023
APPROVAL

ROBERT M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

immediately notified. Immediately alerting building or campus security will also be a prudent step in applicable cases. All persons to whom this Manual applies are reminded that under Section 30 of the DPA, the penalty of imprisonment of one (1) year and six (6) months to five (5) years, and a fine of not less than Five hundred thousand pesos (PhP 500,000.00) but not more than One million pesos (PhP 1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach, and of the obligation to notify the Commission pursuant to Section 20 (f), intentionally or by omission conceals the fact of such security breach.

SECTION 24. The initial security incident or breach notice to be submitted to the proper UP offices (Form 1 https://docs.google.com/document/d/1HC_90nZSoh9ZGaQ2BwhG_Ugs20PNZSv/edit?usp=share_link&oid=100411181806495674654&rtpof=true&sd=true) shall, as far as practicable, indicate the name, office or unit, and contact details of the person reporting the incident or breach, the date and time when the incident or breach occurred or was discovered; the type of data involved (*i. e.*, personal information, sensitive personal information, or other information that may be used to facilitate or enable identity fraud); whether there is reason to believe such information has been acquired by an unauthorized person, and if such acquisition is likely to give rise to a real risk of serious harm to any affected data subject; the approximate number of data subjects or records involved; the possible cause for such incident or breach and extent of such incident or breach; any measures done in order to respond to the incident or breach, and other details that will enable the University authorities concerned to address the threats posed by such incident or breach, and to comply with the applicable provisions of the DPA and NPC issuances.

Since time is of the essence, what is paramount is the giving of immediate notice to the head of unit and/or the ITDC or any other proper IT office, the UP Office of the President and or Chancellor, and the UP System DPO and other proper DPO, through whatever means of communication available, taking into account the circumstances surrounding the security incident or breach. Preliminary verbal notice through a call, or notice through SMS, or other similar means, is permissible but should be followed by a more thorough written notice using Form 1 (such as through secure email) to enable the University offices concerned to properly address and document the incident or breach; comply with applicable laws and requirements of the NPC; and for the purpose of reviewing policies and procedures. A non-member of the UP community may use Form 1 in order to report an incident or breach (*e. g.*, a research participant whose data is involved in an incident or breach). UP personnel who discover that an incident or breach has, or may have, occurred must submit such notice (Form 1) to the concerned head of unit within

Action of the Board of Regents
at its ^{382nd} Meeting on JUN 29 2023
APPROVAL

ROBERTO M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

two (2) hours from the time he or she comes to know of such possible or actual incident or breach.


SECTION 25. Unless a different person is designated by the UP President, or the Chancellor, or his or her authorized representative, in the case of ICT breaches, it is the Director of the Information Technology Development Center (“ITDC”), or CU, or other proper IT office, or, in the case of non-ICT breaches or when the ITDC is not in charge of the affected ICT based system, the head of the office that is responsible for managing the affected system, shall serve as head of the security incident or breach response team. Such head of the security incident or breach response team shall lead the effort and have the authority to make decisions with the assistance of personnel from other UP offices most suited to respond to, mitigate the impact of, and take the appropriate actions in relation to the incident or breach. The security incident or breach response team will likely comprise representatives from various UP System and/or CU offices such as the ITDC, campus security, the head of the office whose ICT-based data processing system was affected, and the Media and Public Relations Office of the Office of the Vice President for Public Affairs or CU information office. The UP System DPO or proper DPO of the unit concerned may or may not be a member of the breach response team. The team shall conduct a preliminary assessment and submit a report using Form 2 (<https://docs.google.com/document/d/1q3mzRTcf7Nc1fntDs2kMETgjGdGsXKVgBmhYnYFeL94/edit?usp=sharing>) for the purpose of:

- (a) Assessing, as far as practicable, the nature and scope of the incident/personal data breach, and the immediate damage or implications of such incident or breach;
- (b) Determining the need for notification of data subjects, the NPC, and/or law enforcement;
- (c) Evaluating the need for external expertise; and
- (d) Implementing immediate measures necessary to secure any evidence, contain the security incident/breach, and restore integrity to the information and communications system.

Since time is of the essence the Director of the ITDC, or other proper IT office, or head of office shall have the authority to seek assistance from relevant UP System and or CU offices. The heads of such UP System or CU offices shall prepare a list of persons whose expertise can immediately be tapped by the ITDC Director or CU IT head, or relevant head of office, when an incident or breach is reported, to serve as members of the latter’s incident or breach response team.

Action of the Board of Regents
at its 32nd Meeting on JUN 29 2023
APPROVAL

ROBERTON L. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

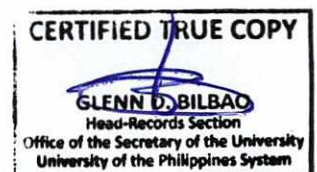
Such head of office shall perform the above functions until such time that he or she receives notice from the UP President or Chancellor that a different person has been designated to exercise such functions.

SECTION 26. The ITDC Director, or CU IT office, or, in the case of non-ICT incidents or breaches or ICT-based systems not being managed by the ITDC, the head of the office responsible for managing the affected system, or such other person designated by the UP President or Chancellor to lead in responding to the incident/breach, shall determine whether the incident or breach can be adequately handled without need of external expertise; that is, expertise outside of the UP System or CU offices. The abovementioned head of office must submit a preliminary assessment report Form 2 (to the UP President or Chancellor, or his or her authorized representative) containing the items mentioned in the prior provision including the description of the breach, action(s) taken to address the breach, the outcome of such action, and such other information that will explain whether UP System or CU offices have the capability to handle and resolve the incident breach, within a period of seventy two (72) hours counted from the time the office acquired knowledge of the breach, either through information provided by personnel of such office or through the notice mentioned in Section 24 above.

In the event such head of office determines that such incident/breach cannot be handled or resolved using internal expertise, the person concerned shall include in the preliminary assessment report (Form 2) a recommendation that the UP President or Chancellor, or his or her duly designated representative, appoint external experts to the breach response team who may be identified by the concerned head of office as members of the incident or breach response team, or for UP to wholly outsource the services of a security incident or breach response team. Since time is of the essence, the preliminary report and recommendation may be done orally or through SMS, or other similar means, but should be followed by a written report (such as through secure email) to enable the University to thoroughly document actions taken in response to the incident or breach, in order to comply with reportorial requirements, and review its policies or procedures.

Concerned UP offices shall prepare a list of external experts, as well as the requirements for the procurement of external expertise, in order to prevent delays in responding to security incidents or data breaches.

A copy of the abovementioned written preliminary assessment report (Form 2) shall also be provided to the UP System DPO and other proper DPO, simultaneously when the said report is transmitted to the UP President or Chancellor, or the latter's authorized representative.



JUL 03 2023

SECTION 27. Within a reasonable time after being notified of the need for external experts to serve as members of the incident or breach response team, or for the functions of such incident or breach response team to be wholly outsourced by the University, the UP President or Chancellor, or his or her authorized representative, with the assistance of relevant offices, shall immediately procure the services of such external experts. Unless a different person is assigned by the UP President or Chancellor, or his or her authorized representative, as head of the team, the head of the IT office or unit whose data was or may have been breached shall continue to serve as the head of the team to which external experts have been appointed, and shall have the authority to make immediate decisions in order to respond to the incident. In the event UP wholly outsources the functions of the data breach response team, such team shall provide periodic reports to the head of the relevant IT office or unit who, in turn, shall provide updates to the UP President or Chancellor. The UP System DPO or other proper DPO, who may or may not be a member of the breach response team, shall assist the University in determining whether there is a duty to notify the NPC and/or the data subjects affected. In cases where the UP System or other proper DPO is not part of the incident or data breach response team, the team head, aside from providing reports to the UP President or Chancellor, or his or her authorized representative, shall provide copies of all reports to the UP System and/or proper DPO.

SECTION 28. The security incident or breach response team shall contain the incident or breach, secure and gather further evidence, determine the need to notify law enforcement, fully evaluate the security incident or personal data breach as to its nature, extent and cause, immediate and long-term damage, impact of the breach, and its potential harm, and negative consequences to affected data subjects. Such team shall likewise see to it that physical and technical measures for responding to an incident or breach address or mitigate the effects of the said incident or breach, are immediately implemented, and shall recommend appropriate organizational measures for the consideration of the relevant UP offices. Relevant UP offices shall provide appropriate assistance to affected data subjects pursuant to the assessment and recommendation of the security incident or breach response team. The team head shall provide periodic written updates to the UP President (or his/her authorized representative), and the UP System and other proper DPO, during the course of responding to and resolving the incident/breach.

SECTION 29. As a rule, the University, through the proper offices mentioned below, shall notify the NPC through the NPC data breach portal at <https://dbnms.privacy.gov.ph/login> and affected data subjects within seventy two (72) hours from knowledge or reasonable belief that sensitive personal information, or other information that may, under the circumstances, be used to enable identity fraud, are reasonably believed to have been

Action of the Board of Regents
at its 382 Meeting on JUN 29 2023
APPROVAL

ROBERT M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

acquired by an unauthorized person, and UP or the NPC believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The term *other information* shall include, but not be limited to, data about the financial or economic situation of the data subject; usernames; passwords and other login data; email addresses; biometric data; copies of identification documents, licenses or unique identifiers like PhilHealth, SSS, GSIS, TIN numbers; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

The head of the office that has access to the best available information pertaining to a data breach (the ITDC Director or other proper IT office head, or, in the case of non-IT breaches or where the affected system is not being managed by the ITDC, the head of the office managing the affected data processing system) shall provide the mandatory notice to affected data subjects within the prescribed period (with the assistance of the DPO and other concerned offices), unless a different person is authorized by the UP President or Chancellor. In order for the proper DPO to provide such assistance and for such proper DPO to report to the NPC through the DBNMS portal <https://dbnms.privacy.gov.ph/login> the office concerned must provide timely and complete information to such DPO using Form 3 (<https://docs.google.com/document/d/1JMKXiqG0DeJ-zmSzoXRrFOLK-4GgBWZ/edit?usp=sharing&oid=100411181806495674654&rtfpof=true&sd=true>) The Office of the UP President or Chancellor, the UP System DPO, and or other concerned DPOs must be provided a copy of the email notices sent to the affected data subjects as well as Form 3.

The head of the office that is undertaking measures to address the data breach must inform the data subjects concerned and the NPC of such measures, as well as any updates regarding the same. If such office is not the office with the duty to provide such notice, the head of office must provide such information in a timely manner to such other office to enable the latter to perform its duty.

SECTION 30. Where there is uncertainty regarding the need for notification, the University shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, can reduce the risks arising from the personal data breach reasonably believed to have occurred.



JUL 03 2023

The University shall also consider if the personal data reasonably believed to have been compromised involves:

- (a) Information that will likely affect national security, public safety, public order, or public health;
- (b) At least one hundred (100) individuals;
- (c) Information required by applicable laws or rules to be confidential; or
- (d) Personal data of vulnerable data subjects such as minors, the mentally ill, asylum seekers, the elderly, patients, those data subjects whose personal data involve criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a personal information controller or personal information processor (as defined under NPC Advisory Opinion 2018-077 and NPC Advisory Opinion 2021-043).

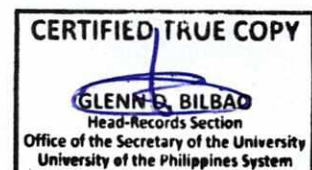
SECTION 31. The proper DPO shall notify the NPC of a personal data breach subject to the following procedures:

31.1. *When Notification Should Be Done.* The NPC shall be notified by the proper DPO through the NPC's data breach portal <https://dbnms.privacy.gov.ph/login> within seventy-two (72) hours upon knowledge of, or the reasonable belief, by UP or its personal information processor that a personal data breach has occurred.

31.2. *Delay in Notification.* Notification may only be delayed to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. UP need not be absolutely certain of the scope of the breach prior to notification. Its inability to immediately secure or restore integrity to the information and communications system shall not be a ground for any delay in notification, if such delay would be prejudicial to the rights of the data subjects. Delay in notification shall not be excused if it is used to perpetuate fraud or to conceal the personal data breach.

31.3. *When Delay is Prohibited.* There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the NPC shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless UP is granted additional time by the NPC to comply.

31.4. *Content of Notification.* The notification shall include, but not be limited to:



JUL 03 2023

1. Nature of the Breach

- (a) description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
- (b) a chronology of the events leading up to the loss of control over the personal data;
- (c) approximate number of data subjects or records involved;
- (d) description or nature of the personal data breach;
- (e) description of the likely consequences of the personal data breach; and
- (f) name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved

- (a) description of sensitive personal information involved; and
- (b) description of other information involved that may be used to enable identity fraud.

3. Measures Taken to Address the Breach

- (a) description of the measures taken or proposed to be taken to address the breach;
- (b) actions being taken to secure or recover the personal data that were compromised;
- (c) actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
- (d) action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
- (e) the measures being taken to prevent a recurrence of the incident.

NPC MC 2016-03 states that the Commission reserves the right to require additional information, if necessary.

31.5. *Form.* Notification shall be in the form of a report (Form 3), whether written or electronic, containing the required contents of notification; *provided*, that the report shall also include the name and contact details of the data protection officer and a designated representative of the University; *provided further*, that, where applicable, the manner of notification of the data subjects shall also be included in the report.



JUL 03 2023

SECTION 32. The concerned office shall notify or cause the UP ITDC or CU IT office, or other relevant office, to send notice to the data subjects affected by a personal data breach, subject to the following procedures:

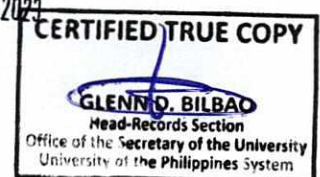
32.1. *When Should Notification Be Done.* The data subjects shall be notified within seventy-two (72) hours upon knowledge of, or reasonable belief by, UP or its personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.

32.2. *Exemption or Postponement of Notification.* If it is not reasonably possible to notify the data subjects within the prescribed period, UP shall request the NPC for an exemption from the notification requirement, or the postponement of the notification. UP may be exempted from the notification requirement where the NPC determines that such notification would not be in the public interest or in the interest of the affected data subjects. The NPC may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of NPC Circular 16-03, and other risks posed by the personal data breach.

32.3. *Content of Notification.* The notification (Form 4 https://docs.google.com/document/d/1VvGkjASTvhB_682SJ9656a6Co09W7aRw/edit?usp=sharing&oid=100411181806495674654&rtpof=true&sd=true)

shall include, but not be limited to:

1. nature of the breach;
2. personal data possibly involved;
3. measures taken to address the breach;
4. measures taken to reduce the harm or negative consequences of the breach;
5. representative of UP, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and



JUL 03 2023

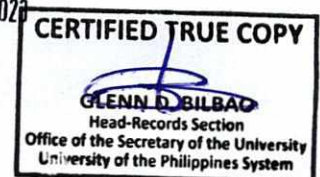
6. any assistance to be provided to the affected data subjects.

Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.

32.4. *Form.* Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The University shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. UP shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach; *provided*, that where individual notification is not possible or would require a disproportionate effort, UP may seek the approval of the NPC to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner; *provided further*, that the University shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.

SECTION 33. All actions taken by the University in responding to a security incident or data breach shall be properly documented. All security incidents and personal data breaches shall be documented through written reports (Form 5 https://docs.google.com/document/d/1FtHhmT_d1sSeo12SfmsdzFEh_8Wwf-6J6O1leZO844/edit?usp=sharing), including those not covered by the notification requirements. All reports from the head of the incident or breach response team should include the following:

- (a) Description of the personal data breach, its root cause, and circumstances regarding its discovery;
- (b) Actions and decisions of the incident response or breach response team. These must be properly documented through written periodic reports and a final report to be prepared by the head of the security incident or breach response team, with the assistance of the data breach response team members. Aside from a narrative report, the measures adopted in order to address the breach need to be documented through, for example, relevant memos, emails, screen shots of actions taken, logs, documents from a relevant third party, sworn statements, and the like. Such report and documentation regarding measures done by an office assisting the head of the breach response team must be provided to concerned officers or offices such as the proper DPO, the UP President, and the head of the breach response team, for the purpose of enabling UP to comply with the DPA and NPC issuances.
- (c) Outcomes of the incident/breach management, and difficulties encountered; and



JUL 03 2023

(d) Compliance with notification requirements and assistance provided to affected data subjects if applicable.

(e) Recommendations to address and prevent similar incidents/breaches which may include the revision of this breach response procedure, other policies and procedures and/or other stakeholder training, etc.

Unless a different period is granted by the UP President and/or the Chancellor, or his or her authorized representative, all reports shall be submitted to the UP President and or Chancellor, or his or her authorized representative, as well as the System and proper DPO, within a period of fifteen (15) days after the security incident or data breach has been handled, and such report shall be made available when requested by the NPC.

For other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. Any or all reports shall be made available when requested by the NPC; *provided*, that a summary of all reports shall be submitted to the NPC annually, comprised of general information including the number of incidents and breach encountered, classified according to their impact on the availability, integrity, or confidentiality of personal data.

SECTION 34. The UP President and/or Chancellor, or his or her authorized representative, shall constitute within fifteen days counted from the deadline in Section 33 above, an independent committee that shall conduct a review of the handling of a security incident or data breach for the purpose of improving these set of procedures for the handling of security incidents or personal data breaches. If no incident or data breach takes place, and unless a different person or persons is/are assigned by the UP President and/or the Chancellor, the UP System DPO and other proper DPOs shall review these set of procedures pursuant to Section 10 of NPC MC 2016-03. The date of the last review and the schedule for the next succeeding review must always be indicated in the documentation of the security incident or data breach response procedures in this Manual.


PART 8. PENALTIES.

SECTION 35. Section 51 of the IRR of the DPA states that:

Any natural or juridical person, or other body involved in the processing of personal data, who fails to comply with the Data Privacy Act and its IRR, and other issuances of the NPC, shall be liable for such violation, and shall be subject to its corresponding sanction, penalty, or fine, without prejudice to any civil or criminal liability, as may be applicable.

Action of the Board of Regents
at its 382nd Meeting on JUN 29 2023
APPROVAL

ROBERT M. TARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN B. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

In cases where a data subject files a complaint for violation of his/her rights as data subject, and for any injury suffered as a result of the processing of his/her personal data, the National Privacy Commission may award indemnity on the basis of the applicable provisions of the New Civil Code.

In case of criminal acts and their corresponding personal penalties, the person who committed the unlawful act or omission shall be recommended for prosecution by the NPC based on substantial evidence. If the offender is a corporation, partnership, or any juridical person, the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime, shall be recommended for prosecution by the National Privacy Commission (“NPC”) based on substantial evidence.

SECTION 36. Aside from the abovementioned criminal and civil sanctions, violations of this Manual may also be the subject of applicable disciplinary proceedings under relevant University or Civil Service rules including the University’s current AUP (and its amendments) and, in the case of students, the applicable student disciplinary code or code of student conduct.

PART 9. EFFECTIVITY AND REVISIONS

SECTION 37. The Board of Regents grants to the UP President the power to issue guidelines for orderly administration of this Manual; charges the said UP President with the duty to publish the same and to submit a copy to the Office of the National Administrative Register of the UP Law Center. This Manual shall take effect immediately after publication at <https://privacy.up.edu.ph/> as there is an urgent need to protect the data privacy of data subjects and this Manual is a codification of already existing laws, rules and issuances arranged in such manner as to enable UP to comply with the PDPA and other applicable laws, rules and regulations.

SECTION 38. Approval by the Board of Regents of this Manual carries with it the authorization from the Board of Regents to the UP President to approve amendments to the same upon the recommendation of the University of the Philippines System Data Privacy Committee which shall be Chaired by the UP System DPO with the Constituent University, Philippine General Hospital and Philippine Genome Center DPOs as members. It is understood that in the event that the Philippine Data Privacy Act, its implementing rules and regulations or National Privacy Commission issuances or any other applicable laws, rules and regulations or issuances as well as jurisprudence interpreting the same are amended that this Manual shall also be deemed accordingly amended.



JUL 03 2023

ANNEXES
FORM 1
UNIVERSITY OF THE PHILIPPINES
INITIAL SECURITY INCIDENT OR DATA BREACH NOTICE FORM

The efficient and effective management of security incidents¹ and data breaches² involving personal data (personal and sensitive personal information) is required in order to ensure

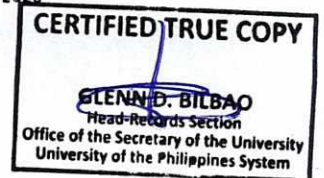
¹ Security incident is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place.

² 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. A personal data breach may be in the nature of:

- (1) An availability breach resulting from loss, accidental or unlawful destruction of personal data;
- (2) Integrity breach resulting from alteration of personal data; and/or
- (3) A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.

UP SYSTEM DATA PRIVACY MANUAL 2023 EDITION

PAGE 47 OF 64



JUL 03 2023

that University of the Philippines System Administration Offices are able to comply with the Philippine Data Privacy Act of 2012, maintain the confidentiality, integrity and security of our processing systems and the data we hold, and ensure mitigating and remedial measures can be put in place promptly so that the rights of data subjects are protected and upheld.


Pursuant to UP's Acceptable Use Policy, this form can be accomplished by any member of the UP community who becomes, or is made aware of a security incident or personal data breach. A non member of the UP community may likewise use this form in order to report an incident or breach e.g. a research participant whose data is involved in an incident or breach. Since time is of the essence, a report may be made via a call to the concerned offices e.g. UP ITDC or the office whose data processing system may have been involved in the incident or breach. It is the authorised personnel of such offices who may fill up the form based on information provided through such call.

This form should be completed (if practicable) as soon as possible and submitted without undue delay to the email addresses below. In the case of personnel of the unit or office whose data processing system is involved in the incident or breach s/he must submit the report within two (2) hours from knowledge or awareness of such an incident or breach. This form must be emailed to the head of the office whose data processing system was affected by the incident or breach (email addresses and office numbers of UP System offices are available at <https://up.edu.ph/up-system-officials-and-offices/>), the UP ITDC CERT@up.edu.ph, the Office of the President op@up.edu.ph and the UP System Data Protection Officer dpo@up.edu.ph. The contact information of Constituent University officials and offices is available through the CU websites. A person reporting such incident or breach is also requested to call the concerned offices to report such incident or breach and thereafter to provide a hard copy of the report to the concerned offices for documentation purposes as well as in cases when UP IT systems are down e.g. UP mail, MS Office email or homegrown CU email services are unavailable. VOIP numbers of UP System offices are available at <https://voip.up.edu.ph/>. Landline office numbers of UP System offices are available at <https://up.edu.ph/up-system-officials-and-offices/>. The UP Office of the President and UP System Data Protection Officer may be contacted via telephone numbers (632) 89280110. The UP ITDC Director may be contacted through telephone numbers 8920-2080 / (632) 8981-8500 local 4469.

As stated above, UP ITDC or other UP personnel may also fill up this form on behalf of a person reporting an incident or breach through a phone call.

Action of the Board of Regents
at its 23rd Meeting on JUN 29 2023
APPROVAL

ROBERT M. LLARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN U. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

Please treat the information contained within this form as strictly confidential. It is UP, through its authorised offices or officials that will inform the affected data subjects as well as the NPC pursuant to the DPA.

I. REPORTING PERSON DETAILS:

Name:

Unit/Office:

Telephone number:

Cellphone number:

Email address:

Your above personal information will be processed by UP for the purpose of efficiently communicating with you regarding the incident or breach and for such other related purposes as allowed by the DPA e.g. providing the relevant information to UP offices tasked with handling the incident or breach as well as law enforcement if necessary.

NOTE: If the above information was filled up by UP ITDC or personnel of other offices in behalf of a person reporting through a call please fill up the following:

Name of UP ITDC or other office staff receiving the report via call:

Unit/Office:

Telephone number:

Cellphone number:

Email address:


Your above personal information will be processed by UP for the purpose of efficiently communicating with you regarding the incident or breach and for such other related purposes as allowed by the DPA e.g. providing the relevant information to UP offices tasked with handling the incident or breach as well as law enforcement if necessary.

II. SECURITY INCIDENT OR DATA BREACH DETAILS:

Time and Date of Incident (you may provide an approximate time and date, indicate earliest approximate time and date possible as this will help uphold the right of data subjects)

Action of the Board of Regents
at its 32nd Meeting on JUN 29 2023
APPROVAL

ROBERTO M. TARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

Data Processing System involved

Type of data involved

Please refer to the definitions in the footnotes below and list all information involved under each category

- a. Personal information (information that can be used to identify an individual including pseudonymized information or information which when put together with other information will identify an individual excluding sensitive personal information)
- b. Sensitive personal information³
- c. Other information that may be used to perpetrate identity fraud⁴

If you are not certain whether information is personal information kindly indicate such pieces of information below⁵:

³ Sensitive personal information refers to personal information:

- (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- (2) 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;
- (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- (4) Specifically established by an executive order or an act of Congress to be kept classified.

⁴ Other information shall include, but not be limited to, data about the financial or economic situation of the data subject; usernames; passwords and other login data; email addresses; biometric data; copies of identification documents, licenses or unique identifiers like PhilHealth, SSS, GSIS, TIN numbers; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

⁵ ... genetic data can only be considered personal data if it can directly identify a specific individual. A genetic sample by itself is not personal data unless it is analyzed to produce data which can identify a specific individual. Similarly, anonymized or aggregated genetic data without any identifiers or which can no longer be related to any specific genetic identity or profile shall not be considered personal data. See NPC Advisory Opinion 2021-23 <https://www.privacy.gov.ph/wp-content/uploads/2021/07/Redacted-Advisory-Opinion-No.-2021-023.pdf>

Action of the Board of Regents
 at its 282 Meeting on JUN 29 2023

APPROVAL

[Signature]

ROBERTO M. TARA
 Secretary of the University
 and of the Board of Regents

CERTIFIED TRUE COPY

[Signature]

GLENN D. BILBAO
 Head-Records Section
 Office of the Secretary of the University
 University of the Philippines System

JUL 03 2023 -

Is there reason to believe such information has been acquired by an unauthorized person ?
___ Yes ___ No ___ Not Sure (check appropriate answer) Please provide details.

Do you think that UP or the National Privacy Commission will consider such acquisition to be likely to give rise to a real risk of serious harm to any affected data subjects ? ___ Yes ___ No ___ Not Sure Please provide details.

Number of data subjects or records involved. Please indicate if you are providing an estimated or approximate number of subjects or records.

Does the incident or breach involve:

(a) Information that will likely affect national security, public safety, public order, or public health ___ Yes ___ No ___ Not Sure

(b) At least one hundred (100) individuals ___ Yes ___ No ___ Not Sure

(c) Information required by applicable laws or rules to be confidential ___ Yes ___ No ___ Not Sure

(d) Personal data of vulnerable groups ⁶ ___ Yes ___ No ___ Not Sure e.g. students, patients, vulnerable research participants ⁷

⁶ Processing operations performed on vulnerable data subjects like minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a personal information controller or personal information processor require special protection. NPC Advisory Opinion 2018-077 and NPC Advisory Opinion 2021-043.

⁷ There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless UP is granted additional time by the Commission to comply.

Action of the Board of Regents
at its 28th Meeting on JUN 29 2023
APPROVAL
[Signature]
ROBERTO M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY
[Signature]
GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

Nature of incident or breach (Does the same involve the confidentiality, integrity or availability of data?)

Cause or possible cause of such incident or breach (Examples dedicated denial of service attack, hacking, phishing, spoofing, loss or theft of equipment or storage media)

If loss of theft of equipment or storage media is involved

- a. Is equipment self or UP owned?

- b. What technical measures, if any, will help prevent unauthorised access e.g. remote wiping⁸, cellphone, laptop or PC is password protected
Are UP files in laptop/PC/storage media e.g. USB, external drive encrypted⁹?

Extent or scope of such incident or breach

Measures done if any to respond to the incident or breach

Other information that will enable the University authorities concerned to address the threats posed by such incident or breach or to evaluate whether or not to notify data subjects and the NPC.

⁸ MC 2016-01, SECTION 21. Remote Disconnection or Deletion. A government agency shall adopt and use technologies that allow the remote disconnection of a mobile device owned by the agency, or the deletion of personal data contained therein, in event such mobile device is lost. A notification system for such loss must also be established.

⁹ MC 2016-01 SECTION 26. Portable Media. A government agency that uses portable media, such as disks or USB drives, to store or transfer personal data must ensure that the data is encrypted. Agencies that use laptops to store personal data must utilize full disk encryption.



JUL 03 2023

- a. Describe how the security incident or breach occurred and the data processing system vulnerability that allowed such security incident or breach
- b. Provide a chronology that describes how the security incident or breach occurred; describe individually the events that led to the loss of control over the personal data.

Recommendations and comments if any


FORM 2
UNIVERSITY OF THE PHILIPPINES
PRELIMINARY ASSESSMENT FORM
FOR SECURITY INCIDENTS OR PERSONAL DATA BREACHES ¹⁰

- I. Nature and scope of the incident/ personal data breach
- II. Immediate damage or implications of such incident or breach (confidentiality, integrity, availability of personal data)

¹⁰ This must be accomplished by the head of the incident or breach response team (either UP ITDC Director or head of unit whose data processing system is affected) and transmitted to the UP President and the UP System Data Protection Officer within a reasonable period of time before the 72 hour period counted from notice of the incident or breach to enable UP to make a timely notice to data subjects and the NPC per NPC MC 2016-03. See Secs. 7 and 8 of the Proposed Security Incident and Personal Data Breach Procedures for UP System Offices

Action of the Board of Regents
at its 382 Meeting on JUN 29 2023
APPROVAL

ROBERTO M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

III. Initial assessment regarding UP’s obligation to notify data subjects and the NPC¹¹
Note that in case of doubt UP must consider whether providing notice to data subjects will enable them to avoid the risk of serious harm¹²

IV. Assessment regarding UP’s obligation to notify law enforcement agencies.¹³

V. Recommendation regarding the need for external expertise (including expertise outside of the UP System Administration Offices but which can be obtained from the CUs e.g. faculty or staff who can conduct forensic examinations)

V. What immediate measures have been taken to:
Secure evidence?

Contain the incident or breach?


¹¹ UP shall notify the NPC and affected data subjects within seventy two (72) hours from knowledge or reasonable belief that sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and UP or the NPC believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. Other information shall include, but not be limited to, data about the financial or economic situation of the data subject; usernames; passwords and other login data; email addresses; biometric data; copies of identification documents, licenses or unique identifiers like PhilHealth, SSS, GSIS, TIN numbers; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

¹² Where there is uncertainty as to the need for notification, the concerned office shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, can reduce the risks arising from the personal data breach reasonably believed to have occurred. Such office shall also consider if the personal data reasonably believed to have been compromised involves: (a) Information that will likely affect national security, public safety, public order, or public health; (b) At least one hundred (100) individuals; (c) Information required by applicable laws or rules to be confidential; or (d) Personal data of vulnerable groups. There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless UP is granted additional time by the Commission to comply.

¹³ https://www.doj.gov.ph/reporting_cybercrime.html
<https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/>
<https://www.officialgazette.gov.ph/2015/08/12/implementing-rules-and-regulations-of-republic-act-no-10175/>

Action of the Board of Regents
at its 382nd Meeting on JUN 29 2023
APPROVAL

ROBERTO M. TARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN B. BILBAS
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

Restore integrity to the ICT system?

FORM 3
UNIVERSITY OF THE PHILIPPINES

UP SYSTEM DATA PRIVACY MANUAL 2023 EDITION

PAGE 55 OF 64

Action of the Board of Regents
at its 282nd Meeting on JUN 29 2023
APPROVAL

ROBERTO M. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

MANDATORY PERSONAL DATA BREACH NOTIFICATION FOR THE NATIONAL PRIVACY COMMISSION¹⁴

General cause (Indicate if due to malicious attack, system glitch, human error or a combination of the same)

Specific cause

Indicate if the notice includes a request to the NPC ie Request for postponement of notification to NPC and/or data subjects, Request for alternative means of informing data subjects See NPC 2016-03

Describe how the breach occurred and the data processing system vulnerability that allowed such breach

Provide a chronology that describes how the breach occurred; describe individually the events that led to the loss of control over the personal data.

¹⁴ Email the accomplished form to the UP System (dpo@up.edu.ph) as well as the proper DPO (PGH, PGC, CU etc) so that the DPO will be able to report to the NPC pursuant to the provisions of the UP Data Privacy Manual

SECTION 30. The concerned office shall notify the NPC of a personal data breach subject to the following procedures:

30.1. When Notification Should Be Done. The NPC shall be notified by the proper DPO through the NPC's data breach portal <https://dbnms.privacy.gov.ph/login> within seventy-two (72) hours upon knowledge of or the reasonable belief by UP or its personal information processor that a personal data breach has occurred.

30.2. Delay in Notification. Notification may only be delayed to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. UP need not be absolutely certain of the scope of the breach prior to notification. Its inability to immediately secure or restore integrity to the information and communications system shall not be a ground for any delay in notification, if such delay would be prejudicial to the rights of the data subjects. Delay in notification shall not be excused if it is used to perpetuate fraud or to conceal the personal data breach.

30.3. When Delay is Prohibited. There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the NPC shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless UP is granted additional time by the NPC to comply.

Action of the Board of Regents
at Its 382 Meeting on JUN 29 2023
APPROVAL

ROBERTO M. J. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN S. BILBAS
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

Approximate number of data subjects or records involved. Does it involve at least 100 data subjects? (Note no postponement of notification is allowed in this case) Provide details to explain the answer.

Provide a description of how the breach will affect UP and the data subjects involved

Indicate the name of the Data Protection Officer or responsible person reporting the breach

Indicate all the sensitive personal information involved¹⁵

Indicate all other information involved that may be used to perpetrate fraud¹⁶

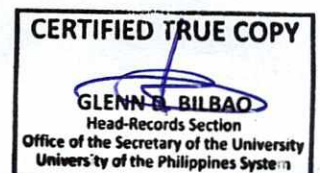
Specific measures to address the breach including the results of the investigation conducted.

Actual measures to secure or recover the personal data involved

¹⁵ Sensitive personal information refers to personal information:

- (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- (2) 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;
- (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- (4) Specifically established by an executive order or an act of Congress to be kept classified.

¹⁶ Other information shall include, but not be limited to, data about the financial or economic situation of the data subject; usernames; passwords and other login data; email addresses; biometric data; copies of identification documents, licenses or unique identifiers like PhilHealth, SSS, GSIS, TIN numbers; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.



JUL 03 2023

Actual measures taken to mitigate harm

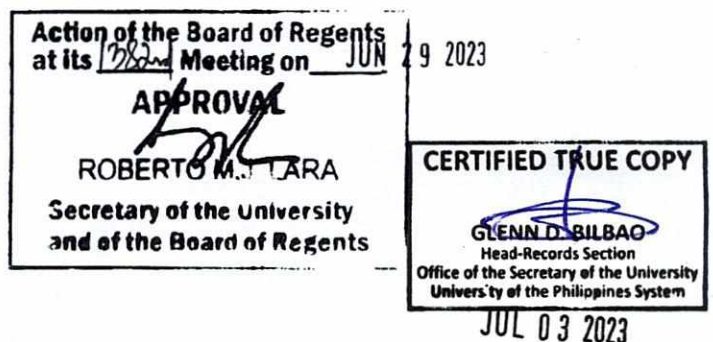
The actual manner used to notify data subjects and including any assistance extended to them

Actual or proposed orientation materials addressing the vulnerability identified

Record type involved (e.g digital or physical, email, email with attachments)

Data subjects involved (Own employees, vulnerable groups e.g. students, research participants¹⁷, customers, etc)

¹⁷ These include minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a personal information controller or personal information processor require special protection. NPC Advisory Opinion 2018-077 and NPC Advisory Opinion 2021-043.



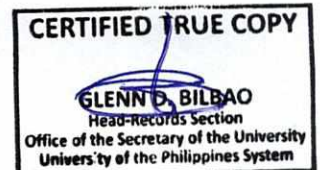
FORM 4
UNIVERSITY OF THE PHILIPPINES
MANDATORY PERSONAL DATA BREACH NOTIFICATION FOR DATA
SUBJECTS

University of the Philippines (insert if System or CU)
Address
Contact information

Insert date

Subject: Data Breach dated (insert date) of (insert data processing system or data base)

Dear (insert name of data subject)



JUL 03 2023

We regret to inform you that your data has been exposed in this data breach. To our understanding, your exposure is limited to: (insert data involved in the data breach)

Nature of the breach

Provide a summary of the events that led up to the loss of control over the data. Do not further expose the data subject

Describe the likely consequences of the personal data breach.

Measures taken to Address the Breach

Provide information on measures taken or proposed to be taken to address the breach, and to secure or recover the personal data that were compromised.

Include actions taken to inform affected individuals of the incident. In case the notification has been delayed, provide reasons.

Describe steps the organization has taken prevent a recurrence of the incident

Measures taken to reduce the harm or negative consequences of the breach.

Describe actions taken to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident. Assistance to be provided to the affected data subjects.

Include information on any assistance to be given to affected individuals.

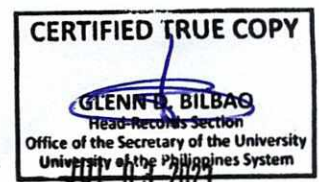
Do not hesitate to contact our Data Protection Officer for further information:

We undertake to provide more information to you as soon as they become available.

Sincerely,

SOURCE: NPC Advisory 2018-02

Please be guided by the following provision in the UP Data Privacy Manual:



SECTION 31. The concerned office shall notify or cause the UP ITDC or CU IT office, or other relevant office, to send notice to the data subjects affected by a personal data breach, subject to the following procedures:

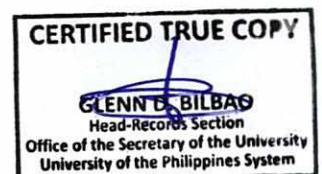
31.1. When Should Notification Be Done. The data subjects shall be notified within seventy-two (72) hours upon knowledge of, or reasonable belief by, UP or its personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.

31.2. Exemption or Postponement of Notification. If it is not reasonably possible to notify the data subjects within the prescribed period, UP shall request the NPC for an exemption from the notification requirement, or the postponement of the notification. UP may be exempted from the notification requirement where the NPC determines that such notification would not be in the public interest or in the interest of the affected data subjects. The NPC may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of NPC Circular 16-03, and other risks posed by the personal data breach.

31.3. Content of Notification. The notification (Form 4) shall include, but not be limited to:

1. nature of the breach;
2. personal data possibly involved;
3. measures taken to address the breach;
4. measures taken to reduce the harm or negative consequences of the breach;
5. representative of UP, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
6. any assistance to be provided to the affected data subjects.

Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.




JUL 03 2023

31.4. Form. Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The University shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. UP shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: Provided, that where individual notification is not possible or would require a disproportionate effort, UP may seek the approval of the NPC to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the University shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.

Action of the Board of Regents
at its ~~282~~ Meeting on JUN 29 2023
APPROVAL

ROBERTO M. TARA
Secretary of the University
and of the Board of Regents

2023

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023

FORM 5
UNIVERSITY OF THE PHILIPPINES
FINAL REPORT OF SECURITY INCIDENT OR PERSONAL DATA BREACH ¹⁸

- I. Description of the security incident or personal data breach, its root cause and circumstances regarding its discovery
- II. Actions and decisions of the incident response or breach response team¹⁹.

¹⁸ The UP Data Privacy Manual states:

SECTION 32. All actions taken by the University in responding to a security incident or data breach shall be properly documented. All security incidents and personal data breaches shall be documented through written reports (Form 5), including those not covered by the notification requirements. ...

All reports shall be submitted to the proper DPO and made available when requested by the NPC:

For other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. Any or all reports shall be made available when requested by the NPC: Provided, that a summary of all reports shall be submitted to the NPC annually, comprised of general information including the number of incidents and breach encountered, classified according to their impact on the availability, integrity, or confidentiality of personal data.

¹⁹ These must be properly documented through written periodic reports and a final report to be prepared by the head of the security incident or breach response team with the assistance of the data breach response team members. Aside from a narrative report, the measures adopted in order to address the breach need to be documented through, for example, relevant memos, emails, screen shots of actions taken, logs, documents from a relevant third party, sworn statements and the like. Such report and documentation regarding measures done by an office assisting the head of the breach response team must be provided to concerned officers or offices such as the proper Data Protection Officer the UP President and the head of the breach response team for the purpose of enabling UP to comply with the Data Privacy Act and National Privacy Commission issuances.



JUL 03 2023

- III. Outcomes of the incident/breach management, and difficulties encountered
- IV. Compliance with notification requirements and assistance provided to affected data subjects if applicable.
- V. Recommendations to address and prevent similar incidents/breaches which may include the revision of this breach response procedure, other policies and procedures, additional stakeholder training, etc.

Action of the Board of Regents
at its 282nd Meeting on JUN 29 2023

APPROVAL

ROBERTON L. LARA
Secretary of the University
and of the Board of Regents

CERTIFIED TRUE COPY

GLENN D. BILBAO
Head-Records Section
Office of the Secretary of the University
University of the Philippines System

JUL 03 2023