UNIVERSITY OF SOUTHERN MINDANAO

COLLEGE OF BUSINESS, DEVELOPMENT ECONOMICS AND MANAGEMENT

ACCOUNTANCY DEPARTMENT

BACHELOR OF SCIENCE IN MANAGEMENT ACCOUNTING





AACCUP LEVEL 1 ACCREDITATION

AREA X
ADMINISTRATION

S.2. The institution has policies and procedures to ensure the security and confidentiality of records.

Freedom of Information

University Of Southern Mindanao

Manual

2017

TABLE OF CONTENTS

1. Overview
    1. Purpose of the Manual
    2. Structure of the Manual
    3. Coverage of the Manual
    4. FOI Receiving Officer
    5. FOI Decision Maker
    6. Central Appeals and Review Committee
    7. Approval and Denial of Request

2. Definition of Terms

3. Protection of Privacy

4. Standard Procedure
    1. Receipt of Request for Information
    2. Initial Evaluation
    a. Request relating to more than one office under the USM
        b. Information is not in the custody of the USM
        c. Requested information already available in USM website
        d. Similar or Identical request for information

    3. Transmittal from FRO to Decision Maker
    4. Role of Decision Maker in processing the Freedom of Information Request
    5. Role of FRO to transmit the Information
    6. Extension of Time
    7. Notifying the requesting party of the decision
    8. Approval of Request
    9. Denial of Request

5. Remedies in Case of Denial of Request

6. Request Tracking System

7. Fees

8. Administrative Liability

9. Annexes
    a. FOI FAQs
    b. Executive Order No. 02
    c. FOI Receiving Officers of the USM and local offices
    d. List of Exceptions to FOI
    e. Flow Chart
    f. FOI Request Form

SECTION 1: OVERVIEW

1. **Purpose:** The purpose of this People's FOI Manual (Manual) is to provide the process to guide and assist Filipino Citizens in requesting for information under Executive Order (E.O.) No. 2, Series of 2016, on Freedom of Information (FOI). (Annex "B")

2. **Structure of the Manual:** This Manual shall set out the rules and procedures to be followed by the UNIVERSITY OF SOUTHERN MINDANAO (USM) when a request for access to information is received. The President is responsible for all actions carried out under this Manual and may delegate this responsibility to the Dr. Lope E. Dapun of Vice President for Administration and Finance of the USM The President may delegate a specific officer to act as the Decision Maker (DM), who shall have overall responsibility for the initial decision on FOI requests, (i.e. to decide whether to release all the records, partially release the records or deny access).

3. **Coverage of the Manual:** The Manual shall cover all requests for information directed to the USM.

4. **FOI Receiving Officer:** There shall be an FOI Receiving Officer (FRO) designated at the USM. The FRO shall preferably come and hold office at PLANNING AND DEVELOPMENT OFFICE.

The functions of the FRO shall include receiving on behalf of the USM all requests for information and forward the same to the appropriate office who has custody of the records; monitor all FOI requests and appeals; provide assistance to the FOI Decision Maker; provide assistance and support to the public and staff with regard to FOI; compile statistical information as required; and, conduct initial evaluation of the request and advise the requesting party whether the request will be forwarded to the FOI Decision Maker for further evaluation, or deny the request based on:

a. That the form is incomplete; or
b. That the information is already disclosed in the USM's Official Website, foi.gov.ph, or at data.gov.ph.

Local offices of the USM shall assign their respective FROs. (Annex "C")

5. **FOI Decision Maker:** There shall be an FOI Decision Maker (FDM), designated by the President, with a rank of not lower than a Division Chief or its equivalent, who shall conduct evaluation of the request for information and has the authority to grant the request, or deny it based on the following:

a. The USM does not have the information requested;
b. The information requested contains sensitive personal information protected by the Data Privacy Act of 2012;
c. The information requested falls under the list of exceptions to FOI; or

d. The request is an unreasonable subsequent identical or substantially similar request from the same requesting party whose request has already been previously granted or denied by the USM.

6. **Central Appeals and Review Committee:** There shall be a central appeals and review committee composed of three (3) officials with a rank not lower than a Director or its equivalent, designated by the President to review and analyze the grant or denial of request of information. The Committee shall also provide expert advice to the President on the denial of such request.

7. **Approval and Denial of Request to Information:** The Decision Maker shall approve or deny all request of information. In case where the Decision Maker is on official leave, the President may delegate such authority to his Chief of Staff or any Officer not below the rank of a Director.

SECTION 2: DEFINITION OF TERMS

CONSULTATION. When a government office locates a record that contains information of interest to another office, it will ask for the views of that other agency on the disclosability of the records before any final determination is made. This process is called a "consultation."

data.gov.ph. The Open Data website that serves as the government's comprehensive portal for all public government data that is searchable, understandable, and accessible.

FOI.gov.ph. The website that serves as the government's comprehensive FOI website for all information on the FOI. Among many other features, FOI.gov.ph provides a central resource for the public to understand the FOI, to locate records that are already available online, and to learn how to make a request for information that is not yet publicly available. FOI.gov.ph also promotes agency accountability for the administration of the FOI by graphically displaying the detailed statistics contained in Annual FOI Reports, so that they can be compared by agency and over time.

EXCEPTIONS. Information that should not be released and disclosed in response to a FOI request because they are protected by the Constitution, laws or jurisprudence.

FREEDOM OF INFORMATION (FOI). The Executive Branch recognizes the right of the people to information on matters of public concern, and adopts and implements a policy of full public disclosure of all its transactions involving public interest, subject to the procedures and limitations provided in Executive Order No. 2. This right is indispensable to the exercise of the right of the people and their organizations to effective and reasonable participation at all levels of social, political and economic decision-making.

FOI CONTACT. The name, address and phone number at each government office where you can make a FOI request

FOI REQUEST. A written request submitted to a government office personally or by email asking for records on any topic. A FOI request can generally be made by any Filipino to any government office.

FOI RECEIVING OFFICE. The primary contact at each agency where the requesting party can call and ask questions about the FOI process or the pending FOI request.

FREQUENTLY REQUESTED INFORMATION. Info released in response to a FOI request that the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records.

FULL DENIAL. When the USM cannot release any records in response to a FOI request, because, for example, the requested information is exempt from disclosure in its entirety or no records responsive to the request could be located.

FULL GRANT. When a government office is able to disclose all records in full in response to a FOI request.

INFORMATION. Shall mean any records, documents, papers, reports, letters, contracts, minutes and transcripts of official meetings, maps, books, photographs, data, research materials, films, sound and video recording, magnetic or other tapes, electronic data, computer stored data, any other like or similar data or materials recorded, stored or archived in whatever format, whether offline or online, which are made, received, or kept in or under the control and custody of any government office pursuant to law, executive order, and rules and regulations or in connection with the performance or transaction of official business by any government office.

INFORMATION FOR DISCLOSURE. Information promoting the awareness and understanding of policies, programs, activities, rules or revisions affecting the public, government agencies, and the community and economy. It also includes information encouraging familiarity with the general operations, thrusts, and programs of the government. In line with the concept of proactive disclosure and open data, these types of information can already be posted to government websites, such as data.gov.ph, without need for written requests from the public.

MULTI-TRACK PROCESSING. A system that divides incoming FOI requests according to their complexity so that simple requests requiring relatively minimal review are placed in one processing track and more complex requests are placed in one or more other tracks. Requests granted expedited processing are placed in yet another track. Requests in each track are processed on a first in/first out basis.

OFFICIAL RECORD/S.Shall refer to information produced or received by a public officer or employee, or by a government office in an official capacity or pursuant to a public function or duty.

OPEN DATA. Refers to publicly available data structured in a way that enables the data to be fully discoverable and usable by end users.

PARTIAL GRANT/PARTIAL DENIAL. When a government office is able to disclose portions of the records in response to a FOI request, but must deny other portions of the request.

PENDING REQUEST OR PENDING APPEAL. An FOI request or administrative appeal for which a government office has not yet taken final action in all respects. It captures anything that is open at a given time including requests that are well within the statutory response time.

PERFECTED REQUEST. A FOI request, which reasonably describes the records, sought and is made in accordance with the government office's regulations.

PERSONAL INFORMATION. Shall refer to any information, whether recorded in a material form or not, from which the identify 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.

PROACTIVE DISCLOSURE. Information made publicly available by government agencies without waiting for a specific FOI request. Government agencies now post on their websites a vast amount of material concerning their functions and mission.

PROCESSED REQUEST OR PROCESSED APPEAL. The number of requests or appeals where the agency has completed its work and sent a final response to the requester.

PUBLIC RECORDS. Shall include information required by laws, executive orders, rules, or regulations to be entered, kept, and made publicly available by a government office.

RECEIVED REQUEST OR RECEIVED APPEAL. An FOI request or administrative appeal that an agency has received within a fiscal year.

REFERRAL. When a government office locates a record that originated with, or is of otherwise primary interest to another agency, it will forward that record to the other agency to process the record and to provide the final determination directly to the requester. This process is called a "referral."

SENSITIVE PERSONAL INFORMATION. As defined in the Data Privacy Act of 2012, shall refer to personal information:

(1) About an individual race, ethnic origin, marital status, age, color, and religious philosophical or political affiliations;

(2) About an individual health, education, genetic or sexual life of a person, or to any proceedings for any offense committed or alleged to have 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.

SIMPLE REQUEST. A FOI request that an agency anticipates will involve a small volume of material or which will be able to be processed relatively quickly.

SECTION 3. PROTECTION OF PRIVACY

While providing for access to information, the USM shall afford full protection to a person's right to privacy, as follows:

a. The USM shall ensure that personal information, particularly sensitive personal information, in its custody or under its control is disclosed only as permited by existing laws;

b. The USM shall protect personal information in its custory or under its control by making reasonable security arrangements against unauthorized access, leaks or premature disclosure;

c. The FRO, FDM, or any employee or official who has access, whether authorized or unauthorized, to personal information in the custody of the USM, shall not disclose that information except as authorized by existing laws.

SECTION 4. STANDARD PROCEDURE (See Annex "E" for flowchart)

1. Receipt of Request for Information.

1.1 The FOI Receiving Officer (FRO) shall receive the request for information from the requesting party and check compliance of the following requirements:

 The request must be in writing;

 The request shall shall state the name and contact information of the requesting party, as well as provide valid proof of identification or authorization; and

 The request shall reasonably describe the information requested, and the reason for, or purpose of, the request for information. (See Annex "F" for request form).

The request can be made through email, provided that the requesting party shall attach in the email a scanned copy of the FOI request form, and a copy of a duly recognized government ID with photo.

1.2 In case the requesting party is unable to make a written request, because of illiteracy or due to being a person with disability, he or she may make an oral request, and the FRO shall reduce it in writing.

1.3 The request shall be stamped received by the FRO, indicating the date and time of the receipt of the written request, and the name, rank, title and position of the public officer who actually received it, with a corresponding signature and a copy, furnished to the requesting party. In case of email requests, the email shall be printed out and shall follow the procedure

mentioned above, and be acknowledged by electronic mail. The FRO shall input the details of the request on the Request Tracking System and allocate a reference number.

1.4 The USM must respond to requests promptly, within the fifteenth (15) working day following the date of receipt of the request. A working day is any day other than a Saturday, Sunday or a day which is declared a national public holiday in the Philippines.In computing for the period, Art. 13 of the New Civil Code shall be observed.

The date of receipt of the request will be either:

a. The day on which the request is physically or electronically delivered to the government office, or directly into the email inbox of a member of staff; or

b. If the government office has asked the requesting party for further details to identify and locate the requested information, the date on which the necessary clarification is received.

An exception to this will be where the request has been emailed to an absent member of staff, and this has generated an 'out of office' message with instructions on how to re-direct the message to another contact. Where this is the case, the date of receipt will be the day the request arrives in the inbox of that contact.

Should the requested information need further details to identify or locate, then the 15 working days will commence the day after it receives the required clarification from the requesting party. If no clarification is received from the requesting party after sixty (60) calendar days, the request shall be closed.

2. Initial Evaluation. After receipt of the request for information, the FRO shall evaluate the contents of the request.

2.1. Request relating to more than one office under the USM: If a request for information is received which requires to be complied with, of different offices, the FRO shall forward such request to the said office concerned and ensure that it is well coordinated and monitor its compliance. The FRO shall also clear with the respective FROs of such offices that they will only provide the specific information that relates to their offices.

2.2. Requested information is not in the custody of the USM or any of its offices: If the requested information is not in the custody of the USM or any of its offices, following referral and discussions with the FDM, the FRO shall undertake the following steps:

 If the records requested refer to another AGENCY, the request will be immediately transferred to such appropriate AGENCY through the most expeditious manner and the transferring office must inform the requesting party that the information is not held within the 15 working day limit. The 15 working day requirement for the receiving office commences the day after it receives the request.

 If the records refer to an office not within the coverage of E.O. No. 2, the requesting party shall be advised accordingly and provided with the contact details of that office, if known.

2.3. Requested information is already posted and available on-line: Should the information being requested is already posted and publicly available in the AGENCY website, data.gov.ph or foi.gov.ph, the FRO shall inform the requesting party of the said fact and provide them the website link where the information is posted.

2.4. Requested information is substantially similar or identical to the previous request: Should the requested information be substantially similar or identical to a previous request by the same requester, the request shall be denied. However, the FRO shall inform the applicant of the reason of such denial.

3. Transmittal of Request by the FRO to the FDM: After receipt of the request for information, the FRO shall evaluate the information being requested, and notify the FDM of such request. The copy of the request shall be forwarded to such FDM within one (1) day from receipt of the written request. The FRO shall record the date, time and name of the FDM who received the request in a record book with the corresponding signature of acknowledgement of receipt of the request.

4. Role of FDM in processing the request: Upon receipt of the request for information from the FRO, the FDM shall assess and clarify the request if necessary. He or she shall make all necessary steps to locate and retrieve the information requested. The FDM shall ensure that the complete information requested be submitted to the FRO within 10 days upon receipt of such request.

The FRO shall note the date and time of receipt of the information from the FDM and report to the AGENCY Head or the designated officer, in case the submission is beyond the 10-day period.

If the FDM needs further details to identify or locate the information, he shall, through the FRO, seek clarification from the requesting party. The clarification shall stop the running of the 15 working day period and will commence the day after it receives the required clarification from the requesting party.

If the FDM determines that a record contains information of interest to another office, the FDM shall consult with the agency concerned on the disclosability of the records before making any final determination.

5. Role of FRO to transmit the information to the requesting party: Upon receipt of the requested information from the FDM, the FRO shall collate and ensure that the information is complete. He shall attach a cover/transmittal letter signed by the USM President or the designated officer and ensure the transmittal of such to the requesting party within 15 working days upon receipt of the request for information.

6. Request for an Extension of Time: If the information requested requires extensive search of the government's office records facilities, examination of voluminous records, the occurrence of fortuitous events or other analogous cases, the FDM should inform the FRO.

The FRO shall inform the requesting party of the extension, setting forth the reasons for such extension. In no case shall the extension exceed twenty (20) working days on top of the mandated fifteen (15) working days to act on the request, unless exceptional circumstances warrant a longer period.

7. Notice to the Requesting Party of the Approval/Denial of the Request: Once the DM approved or denied the request, he shall immediately notify the FRO who shall prepare the response to the requesting party either in writing or by email. All actions on FOI requests, whether approval or denial, shall pass through the USM President or his designated officer for final approval.

8. Approval of Request: In case of approval, the FRO shall ensure that all records that have been retrieved and considered be checked for possible exemptions, prior to actual release. The FRO shall prepare the letter or email informing the requesting party within the prescribed period that the request was granted and be directed to pay the applicable fees, if any.

9. Denial of Request: In case of denial of the request wholly or partially, the FRO shall, within the prescribed period, notify the requesting party of the denial in writing. The notice shall clearly set forth the ground or grounds for denial and the circumstances on which the denial is based. Failure to notify the requesting party of the action taken on the request within the period herein provided shall be deemed a denial of the request to information. All denials on FOI requests shall pass through the Office of the USM President or to his designated officer.

SECTION 5. REMEDIES IN CASE OF DENIAL

A person whose request for access to information has been denied may avail himself of the remedy set forth below:

1. Administrative FOI Appeal to the USM Central Appeals and Review Committee: Provided, that the written appeal must be filed by the same requesting party within fifteen (15) calendar days from the notice of denial or from the lapse of the period to respond to the request.

a. Denial of a request may be appealed by filing a written appeal to the USM Central Appeals and Review Committee within fifteen (15) calendar days from the notice of denial or from the lapse of the period to respond to the request.

b. The appeal shall be decided by the USM President upon the recommendation of the Central Appeals and Review Committee within thirty (30) working days from the filing of said written appeal. Failure to decide within the 30-day period shall be deemed a denial of the appeal.

2. Upon exhaustion of administrative FOI appeal remedies, the requesting party may file the appropriate judicial action in accordance with the Rules of Court.

SECTION 6. REQUEST TRACKING SYSTEM

The USM shall establish a system to trace the status of all requests for information received by it, which may be paper-based, on-line or both.

SECTION 7. FEES

1. No Request Fee. The USM shall not charge any fee for accepting requests for access to information.

2. Reasonable Cost of Reproduction, Copying, and/or Delivery of the Information: The FRO shall immediately notify the requesting party in case there shall be a reproduction, copying and/or delivery fee in order to provide the information. Such fee shall be the actual amount spent by the USM in providing the information to the requesting party. The schedule of fees shall be posted by the USM.

3. Exemption from Fees: The USM may exempt any requesting party from payment of fees, upon request stating the valid reason why such requesting party shall not pay the fee.

SECTION 8. ADMINISTRATIVE LIABILITY

1. Non-compliance with FOI. Failure to comply with the provisions of this Manual shall be a ground for the following administrative pe nalties:

a. 1st Offense - Reprimand;

b. 2nd Offense - Suspension of one (1) to thirty (30) days; and

c. 3rd Offense - Dismissal from the service.

2. Procedure. The Revised Rules on Administrative Cases in the Civil Service shall be applicable in the disposition of cases under this Manual.

3. Provisions for More Stringent Laws, Rules and Regulations. Nothing in this Manual shall be construed to derogate from any law, any rules, or regulation prescribed by any body or agency, which provides for more stringent penalties.

ANNEX "A"

FOI FREQUENTLY ASKED QUESTIONS

Introduction to FOI

1. What is FOI?

Freedom of Information (FOI) is the government's response to the call for transparency and full public disclosure of information. FOI is a government mechanism which allows Filipino citizens to request any information about the government transactions and operations, provided that it shall not put into jeopardy privacy and matters of national security.

The FOI mechanism for the Executive Branch is enabled via Executive Order No. 2, series of 2016.

2. What is Executive Order No. 2 S. 2016?

Executive Order No. 2 is the enabling order for FOI. EO 2 operationalizes in the Executive Branch the People's Constitutional right to information. EO 2 also provides the State policies to full public disclosure and transparency in the public service.

EO 2 was signed by President Rodrigo Roa Duterte on July 23, 2016.

3. Who oversees the implementation of EO 2?

The Presidential Communications Operations Office (PCOO) oversees the operation of the FOI program. PCOO serves as the coordinator of all government agencies to ensure that the FOI program is properly implemented.

Making a Request

4. Who can make an FOI request?

Any Filipino citizen can make an FOI Request. As a matter of policy, requestors are required to present proof of identification.

5. What can I ask for under EO on FOI?

Information, official records, public records, and, documents and papers pertaining to official acts, transactions or decisions, as well as to government research data used as basis for policy development.

6. What agencies can we ask information?

An FOI request under EO 2 can be made before all government offices under the Executive Branch, including government owned or controlled corporations (GOCCs) and state universities and colleges (SUCs).

FOI requests must be sent to the specific agency of interest, to be received by its respective Receiving Officer.

7. How do I make an FOI request?

a. The requestor is to fill up a request form and submits to the agency's Receiving Officer. The Receiving Officer shall validate the request and logs it accordingly on the FOI tracker.

b. If deemed necessary, the Receiving Officer may clarify the request on the same day it was filed, such as specifying the information requested, and providing other assistance needed by the Requestor.

c. The request is forwarded to the Decision Maker for proper assessment. The Decision Maker shall check if the agency holds the information requested, if it is already accessible, or if the request is a repeat of any previous request.

d. The request shall be forwarded to the officials involved to locate the requested information.

e. Once all relevant information is retrieved, officials will check if any exemptions apply, and will recommend appropriate response to the request.

f. If necessary, the head of the agency shall provide clearance to the response.

g. The agency shall prepare the information for release, based on the desired format of the Requestor. It shall be sent to the Requestor depending on the receipt preference.

8. How much does it cost to make an FOI request?

There are no fees to make a request. But the agency may charge a reasonable fee for necessary costs, including costs of printing, reproduction and/or photocopying.

9. What will I receive in response to an FOI request?

You will be receiving a response either granting or denying your request.

If the request is granted, the information requested will be attached, using a format that you specified. Otherwise, the agency will explain why the request was denied.

10. How long will it take before I get a response?

It is mandated that all replies shall be sent fifteen (15) working days after the receipt of the request. The agency will be sending a response, informing of an extension of processing period no longer than twenty (20) working days, should the need arise.

11. What if I never get a response?

If the agency fails to provide a response within the required fifteen (15) working days, the Requestor may write an appeal letter to the Central Appeals and Review Committee within fifteen (15) calendar days from the lapse of required response period. The appeal shall be decided within thirty (30) working days by the Central Appeals and Review Committee.

If all administrative remedies are exhausted and no resolution is provided, requestors may file the appropriate case in the proper courts in accordance with the Rules of Court.

12. What will happen if my request is not granted?

If you are not satisfied with the response, the Requestor may write an appeal letter to the Central Appeals and Review Committee within fifteen (15) calendar days from the lapse of required response period. The appeal shall be decided within thirty (30) working days by the Central Appeals and Review Committee.

If all administrative remedies are exhausted and no resolution is provided, requestors may file the appropriate case in the proper courts in accordance with the Rules of Court.

ANNEX "B"

MALACAÑAN PALACE
MANILA
BY THE PRESIDENT OF THE PHILIPPINES
EXECUTIVE ORDER NO. 02

OPERATIONALIZING IN THE EXECUTIVE BRANCH THE PEOPLE'S CONSTITUTIONAL RIGHT TO INFORMATION AND THE STATE POLICIES TO FULL PUBLIC DISCLOSURE AND TRANSPARENCY IN THE PUBLIC SERVICE AND PROVIDING GUIDELINES THEREFOR

WHEREAS, pursuant to Article 28, Article II of the 1987 Constitution, the State adopts and implements a policy of full public disclosure of all its transactions involving public interest, subject to reasonable conditions prescribed by law;

WHEREAS, Section 7, Article III of the Constitution guarantees the right of the people to information on matters of public concern;

WHEREAS, the incorporation of this right in the Constitution is a recognition of the fundamental role of free and open exchange of information in a democracy, meant to enhance transparency and accountability in government official acts, transactions, or decisions;

WHEREAS, the Executive Branch recognizes the urgent need to operationalize these Constitutional provisions;

WHEREAS, the President, under Section 17, Article VII of the Constitution, has control over all executive AGENCYs, bureaus and offices, and the duty to ensure that the laws be faithfully executed;

WHEREAS, the Data Privacy Act of 2012 (R.A. 10173), including its implementing Rules and Regulations, strengthens the fundamental human right of privacy, and of communication while ensuring the free flow of information to promote innovation and growth;

NOW, THEREFORE, I, RODRIGO ROA DUTERTE, President of the Philippines, by virtue of the powers vested in me by the Constitution and existing laws, do hereby order:

SECTION 1. Definition. For the purpose of this Executive Order, the following terms shall mean:

(a) "Information" shall mean any records, documents, papers, reports, letters, contracts, minutes and transcripts of official meetings, maps, books, photographs,

data, research materials, films, sound and video recording, magnetic or other tapes, electronic data, computer stored data, any other like or similar data or materials recorded, stored or archived in whatever format, whether offline or online, which are made, received, or kept in

or under the control and custody of any government office pursuant to law, executive order, and rules and regulations or in connection with the performance or transaction of official business by any government office.

(b) "Official record/records" shall refer to information produced or received by a public officer or employee, or by a government office in an official capacity or pursuant to a public function or duty.

(c) "Public record/records" shall include information required by laws, executive orders, rules, or regulations to be entered, kept and made publicly available by a government office.

SECTION 2. Coverage. This order shall cover all government offices under the Executive Branch, including but not limited to the national government and all its offices, AGENCYs, bureaus, offices, and instrumentalities, including government-owned or -controlled corporations, and state universities and colleges. Local government units (LGUs) are encouraged to observe and be guided by this Order.

SECTION 3. Access to information. Every Filipino shall have access to information, official records, public records and to documents and papers pertaining to official acts, transactions or decisions, as well as to government research data used as basis for policy development.

SECTION 4. Exception. Access to information shall be denied when the information falls under any of the exceptions enshrined in the Constitution, existing law or jurisprudence.

The AGENCY of Justice and the Office of the Solicitor General are hereby directed to prepare an inventory of such exceptions and submit the same to the Office of the President within thirty (30) calendar days from the date of effectivity of this Order.

The Office of the President shall thereafter, immediately circularize the inventory of exceptions for the guidance of all government offices and instrumentalities covered by this Order and the general public.

Said inventory of exceptions shall periodically be updated to properly reflect any change in existing law and jurisprudence and the AGENCY of Justice and the Office of the Solicitor General are directed to update the inventory of exceptions as the need to do so arises, for circularization as hereinabove stated.

SECTION 5. Availability of SALN. Subject to the provisions contained in Sections 3 and 4 of this Order, all public officials are reminded of their obligation to file and make available for scrutiny their Statements of Assets, Liabilities and Net Worth (SALN) in accordance with existing laws, rules and regulations, and the spirit and letter of this Order.

SECTION 6. Application and Interpretation. There shall be a legal presumption in favor of access to information, public records and official records. No request for information shall be denied unless it clearly falls under any of the exceptions listed in the inventory or updated inventory of exceptions circularized by the Office of the President provided in the preceding section.

The determination of the applicability of any of the exceptions to the request shall be the responsibility of the Head of the Office, which is in custody or control of the information, public record or official record, or the responsible central or field officer duly designated by him in writing.

In making such determination, the Head of the Office or his designated officer shall exercise reasonable diligence to ensure that no exception shall be used or availed of to deny any request for information or access to public records, or official records if the denial is intended primarily and purposely to cover up a crime, wrongdoing, graft or corruption.

SECTION 7. Protection of Privacy. While providing access to information, public records, and official records, responsible officials shall afford full protection to the right to privacy of the individual as follows:

(a) Each government office per Section 2 hereof shall ensure that personal information in its custody or under its control is disclosed or released only if it is material or relevant to the subject matter of the request and its disclosure is permissible under this order or existing law, rules or regulations;

(b) Each government office must protect personal information in its custody or control by making reasonable security arrangements against leaks or premature disclosure of personal information, which unduly exposes the individual, whose personal information is requested, to vilification, harassment or any other wrongful acts.

(c) Any employee, official or director of a government office per Section 2 hereof who has access, authorized or unauthorized, to personal information in the custody of the office, must not disclose that information except when authorized under this order or pursuant to existing laws, rules or regulation.

SECTION 8. People's Freedom to Information (FOI) Manual. For the effective implementation of this Order, every government office is directed to prepare within one hundred twenty (120) calendar days from the effectivity of this Order, its own People's FOI Manual, which shall include among others the following provisions:

(a) The location and contact information of the head, regional, provincial, and field offices, and other established places where the public can obtain information or submit requests;

(b) The person or office responsible for receiving requests for information;

(c) The procedure for the filing and processing of the request as specified in the succeeding section 9 of this Order.

(d) The standard forms for the submission of requests and for the proper acknowledgment of requests;

(e) The process for the disposition of requests;

(f) The procedure for the administrative appeal of any denial for access to information; and

(g) The schedule of applicable fees.

SECTION 9. Procedure. The following procedure shall govern the filing and processing of request for access to information:

(a) Any person who requests access to information shall submit a written request to the government office concerned. The request shall state the name and contact information of the requesting party, provide valid proof of his identification or authorization, reasonably describe the information requested, and the reason for, or purpose of, the request for information: Provided, that no request shall be denied or refused acceptance unless the reason for the request is contrary to law, existing rules and regulations or it is one of the exceptions contained in the inventory or updated inventory of exception as hereinabove provided.

(b) The public official receiving the request shall provide reasonable assistance, free of charge, to enable, to enable all requesting parties and particularly those with special needs, to comply with the request requirements under this Section.

(c) The request shall be stamped by the government office, indicating the date and time of receipt and the name, rank, title and position of the receiving public officer or employee with the corresponding signature, and a copy thereof furnished to the requesting party. Each government office shall establish a system to trace the status of all requests for information received by it.

(d) The government office shall respond to a request fully compliant with requirements of sub-section (a) hereof as soon as practicable but not exceeding fifteen (15) working days from the receipt thereof. The response mentioned above refers to the decision of the agency or office concerned to grant or deny access to the information requested.

(e) The period to respond may be extended whenever the information requested requires extensive search of the government office's records facilities, examination of voluminous records, the occurrence of fortuitous cases or other analogous cases. The government office shall notify the person making the request of the extension, setting forth the reasons for such extension. In no case shall the extension go beyond twenty (20) working days unless exceptional circumstances warrant a longer period.

(f) Once a decision is made to grant the request, the person making the request shall be notified of such decision and directed to pay any applicable fees.

SECTION 10. Fees. Government offices shall not charge any fee for accepting requests for access to information. They may, however, charge a reasonable fee to reimburse necessary costs, including actual costs of reproduction and copying of the information required, subject to existing rules and regulations. In no case shall the applicable fees be so onerous as to defeat the purpose of this Order.

SECTION 11. Identical or Substantially Similar Requests. The government office shall not be required to act upon an unreasonable subsequent identical or substantially similar request from the same requesting party whose request from the same requesting party whose request has already been previously granted or denied by the same government office.

SECTION 12. Notice of Denial. If the government office decides to deny the request, in whole or in part, it shall as soon as practicable, in any case within fifteen (15) working days from the receipt of the request, notify the requesting party the denial in writing. The notice shall clearly set forth the ground or grounds for denial and the circumstances on which the denial is based. Failure to notify the requesting party of the action taken on the request within the period herein stipulated shall be deemed a denial of the request for access to information.

SECTION 13. Remedies in Cases of Denial of Request for Access to Information.

(a) Denial of any request for access to information may be appealed to the person or office next higher in the authority, following the procedure mentioned in Section 9 of this Order: Provided, that the written appeal must be filed by the same person making the request within fifteen (15) calendar days from the notice of denial or from the lapse of the relevant period to respond to the request.

(b) The appeal be decided by the person or office next higher in authority within thirty (30) working days from the filing of said written appeal. Failure of such person or office to decide within the afore-stated period shall be deemed a denial of the appeal.

(c) Upon exhaustion of administrative appeal remedies, the requesting part may file the appropriate case in the proper courts in accordance with the Rules of Court.

SECTION 14. Keeping of Records. Subject to existing laws, rules, and regulations, government offices shall create and/or maintain accurate and reasonably complete records of important information in appropriate formats, and implement a records management system that facilitates easy identification, retrieval and communication of information to the public.

SECTION 15. Administrative Liability. Failure to comply with the provisions of this Order may be a ground for administrative and disciplinary sanctions against any erring public officer or employee as provided under existing laws or regulations.

SECTION 16. Implementing Details. All government offices in the Executive Branch are directed to formulate their respective implementing details taking into consideration their mandates and the nature of information in their custody or control, within one hundred twenty (120) days from the effectivity of this Order.

SECTION 17. Separability Clause. If any section or part of this Order is held unconstitutional or invalid, the other sections or provisions not otherwise affected shall remain in full force or effect.

SECTION 18. Repealing Clause. All orders, rules and regulations, issuances or any part thereof inconsistent with the provisions of this Executive Order are hereby repealed, amended or modified accordingly: Provided, that the provisions of Memorandum Circular No. 78 (s. 1964), as amended, shall not be deemed repealed pending further review.

SECTION 19. Effectivity. This Order shall take effect immediately upon publication in a newspaper of general circulation.

DONE, in the City of Manila, this 23rd day of July in the year of our Lord two thousand and sixteen.

(Sgd.) RODRIGO ROA DUTERTE
President of the Philippines

By the President:

(Sgd.) SALVADOR C. MEDIALDEA
Executive Secretary

ANNEX "C"

FOI Receiving Officers of the AGENCY and its local offices

Name of Office	Location of FOI Receiving Office	Contact Details	Assigned FOI Receiving Officer
PLANNING AND DEVELOPMENT OFFICE	ADMINISTRATION BUILDING, USM, KABACAN, COTABATO	(064)572-2605	DR. EIMER M. ESTILLOSO

ANNEX "D"

LIST OF EXCEPTIONS

The following are the exceptions to the right of access to information, as recognized by the Constitution, existing laws, or jurisprudence: These exceptions only apply to governmental bodies within the control and supervision of the Executive department. Unless specifically identified, these exceptions may be invoked by all officials, officers, or employees in the Executive branch in possession of the relevant records or information.

1. Information covered by Executive privilege;

2. Privileged information relating to national security, defense or international relations;

3. Information concerning law enforcement and protection of public and personal safety;

4. Information deemed confidential for the protection of the privacy of persons and certain individuals such as minors, victims of crimes, or the accused;

5. Information, documents or records known by reason of official capacity and are deemed as confidential, including those submitted or disclosed by entities to government agencies, tribunals, boards, or officers, in relation to the performance of their functions, or to inquiries or investigation conducted by them in the exercise of their administrative, regulatory or quasi-judicial powers;

6. Prejudicial premature disclosure;

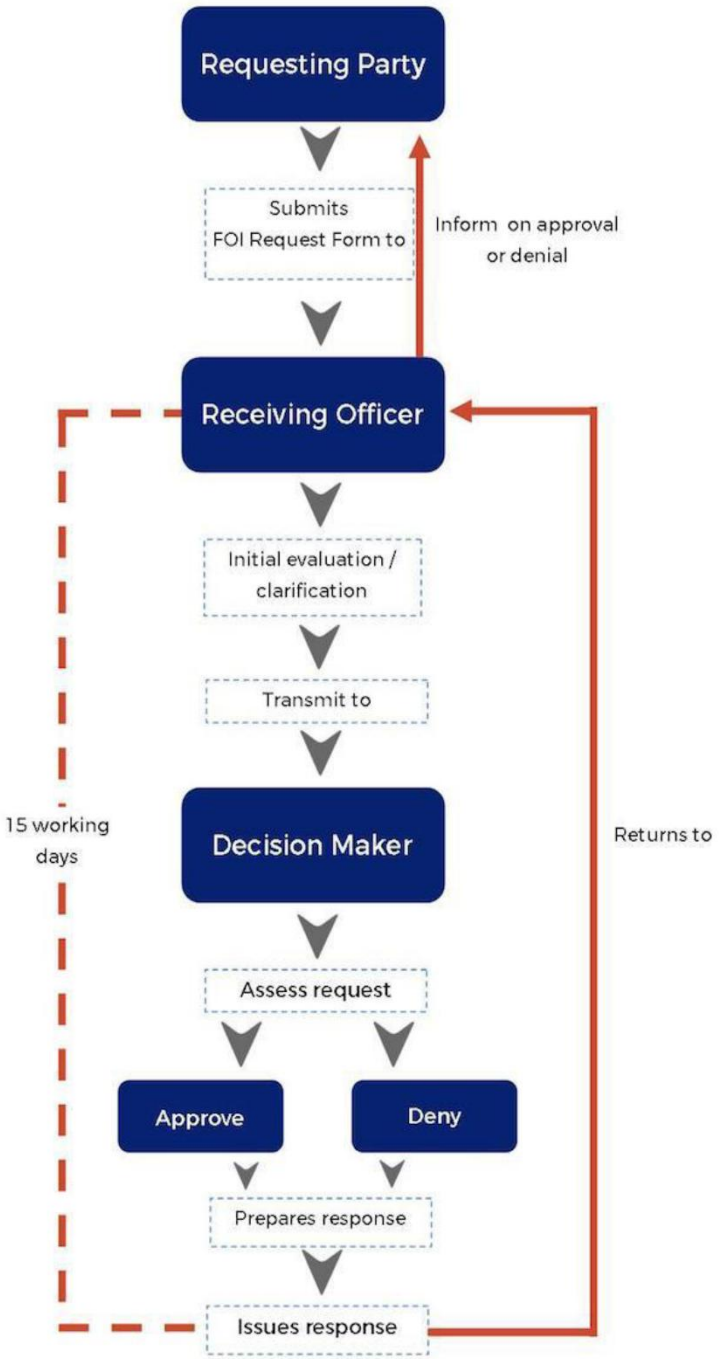
7. Records of proceedings or information from proceedings which, pursuant to law or relevant rules and regulations, are treated as confidential or privileged;

8. Matters considered confidential under banking and finance laws, and their amendatory laws; and

9. Other exceptions to the right to information under laws, jurisprudence, rules and regulations.

ANNEX "E"

Flow Chart



ANNEX "F"

FOI Request Form

This document may be reproduced and is NOT FOR SALE

FOI Tracking Number:

FREEDOM OF INFORMATION REQUEST FORM

(Pursuant to Executive Order No. 2,s. 2016)
(as of November 2016)

Please read the following information carefully before proceeding with your application. Use blue or black ink. Write neatly and in BLOCK letters. Improper or incorrectly-filled out forms will not be acted upon. Tick or mark boxes with "X" where necessary. Note: (◄) denotes a MANDATORY field.

A. Requesting Party

You are required to supply your name and address for correspondence. Additional contact details will help us deal with your application and correspond with you in the manner you prefer.

1. Title *(e.g. Mr, Mrs, Ms, Miss)* 2. Given Name/s *(including M.I)* 3. Surname

4. Complete Address *(Apt/House Number, Street, City/Municipality, Province)*

5. Landline/Fax 6. Mobile 7. Email

8. Preferred Mode of Communication ☐ Landline ☐ Mobile Number ☐ Email ☐ Postal Address
(If your request is successful, we will be sending the documents to you in this manner.)

9. Preferred Mode of Reply ☐ Email ☐ Fax ☐ Postal Address ☐ Pick-Up at Agency

10. Type of ID Given *(Please ensure your IDs contain your photo and signature)* ☐ Passport ☐ Driver's License ☐ SSS ID ☐ Postal ID ☐ Voter's ID ☐ School ID ☐ Company ID ☐ Others

B. Requested Information

11. Agency - Connecting Agency *(if applicable)*

12. Title of Document/Record Requested *(Please be as detailed as possible)*

13. Date or Period *(DD/MM/YY)*

14. Purpose

15. Document Type

16. Reference Numbers *(if known)*

17. Any other Relevant Information

FREEDOM OF INFORMATION

C. Declaration

Privacy Notice: Once deemed valid, your information from your application will be used by the agency you have applied to, to deal with your application as set out in the Freedom of Information Executive Order No. 2. If the Department or Agency gives you access to a document, and if the document contains no personal information about you, the document will be published online in the Department's or Agency's disclosure log, along with your name and the date you applied, and, if another person, company or body will use or benefit from the documents sought, the name of that person,entity or body.

I declare that:
- The information provided in the form is complete and correct;
- I have read the Privacy notice;
- I have presented at least one (1) government-issued ID to establish proof of my identity

I understand that it is an offense to give misleading information about my identity, and that doing so may result in a decision to refuse to process my application.

Signature _____

Date Accomplished *(DD/MM/YYYY)* _____

D. FOI Receiving Officer [INTERNAL USE ONLY]

Name *(Print name)* _____

Agency - Connecting Agency *(if applicable, otherwise N/A)* _____ _____

Date entered on eFOI *(if applicable, otherwise N/A)* _____

Proof of ID Presented *(Photocopies of original should be attached)* ☐ Passport ☐ Driver's License ☐ SSS ID ☐ Postal ID ☐ Voter's ID ☐ School ID ☐ Company ID ☐ Others _____

The request is recommended to be: ☐ Approved ☐ Denied

If Denied, please tick the Reason for the Denial ☐ Invalid Request ☐ Incomplete ☐ Data already available online

Second Receiving Officer Assigned *(print name)* _____

Decision Maker Assigned to Application *(print name)* _____

Decision on Application ☐ Successful ☐ Partially Successful ☐ Denied ☐ Cost

If Denied, please tick the Reason for the Denial ☐ Invalid Request ☐ Incomplete ☐ Data already available online ☐ Exception Which Exception? _____

Date Request Finished *(DD/MM/YYYY)* _____

Date Documents (if any) Sent *(DD/MM/YYYY)* _____

FOI Registry Accomplished ☐ Yes ☐ No

RO Signature _____

Date *(DD/MM/YYYY)* _____

UNIVERSITY OF SOUTHERN MINDANAO
Kabacan, Cotabato

DATA PRIVACY MANUAL

MARCH 2020
(BOR Resolution No 13, s. 2020)

UNIVERSITY OF SOUTHERN MINDANAO
DATA PRIVACY MANUAL

TABLE OF CONTENTS

I. Introduction
II. Privacy Policy Statements
III. Definition of Terms
IV. Scope and Limitations
V. Collection of Personal Information
A. Privacy Principles
1. Transparency
2. Proportionality
3. Legitimate Purpose
B. Provisions for Units in the University
1. Admission and Records Office (ARO)
2. Human Resources Management and Development Office (HRMDO)
3. University Hospital
4. University Guidance Center (UGC)
5. University Information and Communications Technology Office (UICTO)
6. Records Section
7. Other Units
C. Privacy Policies
1. Notification of and Securing Consent from Data Subjects
2. Policy on Access to Personal Information
3. Policy on Information Gathered
VI. Use and Disclosure of Information
A. Primary Purpose
B. Secondary Purposes
C. Policy on Sensitive Personal Information
D. Government Related Use and Disclosure of Personal Information
VII. Ensuring and Maintaining Accuracy of Information
A. Verification of Information
B. Correction and updating of Information
VIII. Security of Personal Information
A. Security Measures
1. Technical Measures
2. Physical Measures
B. Request for Access
C. Retention and Destruction of Personal Information
IX. Inquiry and Complaints
A. Inquiry on Data Privacy Issues
B. Procedure for Complaints for Breach, Loss, or Unauthorized Access, Disclosure or Destruction of Personal Information
X. Effectivity
XI. Annexes
A. DATA PRIVACY NOTICE
B. CONSENT FORM FOR STUDENTS OF THE UNIVERSITY
C. DATA INQUIRY/ACCESS REQUEST FORM
D. NON-DISCLOSURE AGREEMENT FOR EMPLOYEES OF THE UNIVERSITY
E. IMPLEMENTING RULES AND REGULATIONS OF THE DATA PRIVACY ACT OF 2012 REPUBLIC OF THE PHILIPPINES

I. INTRODUCTION

This Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and other relevant policies, including issuances of the National Privacy Commission. The aim of the DPA is to protect personal data in information and communications systems in both the government and private sector.

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

This Manual informs the USM community and the general public of the privacy and data protection protocols carried out within USM for specific circumstances in the lifecycle of the personal data, from collection to destruction, and serves as a guide in for data subjects to exercise their rights under the Data Privacy Act of 2012.=

USM commits to protect the privacy rights of individuals on personal information pursuant to the provisions of Republic Act No. 10173 or the Data Privacy Act of 2012, and its Implementing Rules and Regulations.

All employees, students and administration officers are enjoined to comply with and to share in the responsibility to secure and protect personal information collected and processed by the University of Southern Mindanao in pursuit of legitimate purposes.

II. PRIVACY POLICY STATEMENT

1. USM adheres to the principles of transparency, legitimate purpose and proportionality in the collection, processing, securing, retention and disposal of personal information.
2. The students, parents, guardians, faculty members, employees or third parties whose personal information is being collected shall be considered as data subjects for purposes of these policies.
3. USM upholds the following rights of its data subjects:
    a. to be informed of the reason or purpose of collecting and processing of their personal data
    b. to object or withhold consent for the collection of their personal data, especially in cases of amendments in the use of their personal data and under conditions allowed by privacy and education laws
    c. to be granted access to their personal data that were processed, as well as the names of the recipients of data, manner and sources from which the data were obtained
    d. to correct the information especially in cases of erroneous or outdated data, and to object to collection of personal information within the bounds allowed by privacy and education laws.
    e. to file a complaint and to be granted damages in case of breach or unauthorized access of his personal information.
    f. to erasure or blocking of personal data, to withdraw or order the destruction of their data from the system if there is substantial proof that the provisions of his consent were violated.
4. USM shall secure the personal information of students, parents, guardians, employees and third parties from whom personal information is collected and shall take adequate measures to secure both physical and digital copies of the information.
5. USM shall ensure that personal information is collected and processed only by authorized personnel for legitimate purposes of the University.
6. Any information that is declared obsolete based on the internal privacy and retention procedures of the University shall be disposed of in a secure and legal manner.

7. Any suspected or actual breach of the USM Data Privacy Policy must be reported to any member of the Breach Incident Response Team (BIRT) in accordance with the procedure provided in Section IX (ii) of this Manual.
8. Data subjects may inquire or request for information from the Data Privacy Response Team regarding any matter relating to the processing of their personal data under the custody of USM, including the data privacy and security policies implemented to ensure the protection of their personal data pursuant to Section IX (i) of this Manual.

III. DEFINITION OF TERMS

1. **Authorized personnel** refer to employees or officers of the University specifically authorized to collect and/ or to process personal information either by their function of their office or position, or through specific authority given in accordance with the policies of the University.

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

3. **Data subject** refers to an individual whose personal, sensitive personal, or privileged information is processed. For purposes of this Manual, it refers to officers, employees, students, and third parties whose information is being collected and processed by the University (i.e. applicants for admission or employment, former students or alumni whose records are required by law to be kept and maintained by the University).

4. **Data Protection Officer or DPO** refers to the University officer designated to monitor and ensure the implementation of the Data Privacy policies of the University. The DPO is also the de facto head of the Data Privacy Response Team.

5. **Data Privacy Response Team** refers to the group of persons designated to respond to inquiries and complaints relating to data privacy and to assist in the monitoring and implementation of the Data Privacy policy of the University. The USM Data Privacy Response Team is composed of the Data Privacy Officer and the Personal Information Processors.

6. **Personal data** refers to all types of personal information collected and processed by the University from the data subjects.

7. **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.

8. **Personal Data Classification** refers to the categories of personal information collected and processed by USM. Personal data is classified as follows:

   A. **Public**- These are information readily available and may be disclosed to the public. Examples: Directory of USM offices, course catalogs, program offerings, names of officers, deans and faculty as stated in the Administration portion of the USM website, published researches containing the names of faculty members and students.

   B. **Confidential**- These are information which are declared confidential by law or policy of USM, and which may only be processed by authorized personnel and if disclosed, may cause material harm to the University, or information is sensitive in nature and will affect the health or well-being of the individual.

      Examples:

Employee and student names, addresses, contact numbers, GSIS, SSS, PhilHealth, Passport numbers, student and employee's health information, student counselling and medical records; financial information of parents and students and employees, and student records, employee 201 files and the information contained therein.

C. **Classified**- These are information the access of which is highly restricted, and if disclosed may cause severe or serious harm or injury to the employee, student or third party.

Examples:
Employee and student USM accounts or computer passwords (Data Privacy Law, Anti-Cyber Crime Law, USM IT policies), bank account numbers, PIN numbers of employee and student ATM numbers, if applicable.

9. **Personal information** refers to any information, whether recorded in a material or digital form, 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.

9. **Personal Information Controller or PIC** refers to the University as the entity which controls of the processing of personal data, or instructs another to process personal data on its behalf.

10. **Personal Information Processor or PIP** refers to the person designated as such to whom the personal information controller instructs the processing of personal data pertaining to a data subject.

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

13. **Privacy Statement** is a notification or statement provided to data subjects informing them of the use and purpose for collecting or processing their information, and/or which allows such individual to consent to such processing of information.

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

15. **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 would result to a personal data breach.

16. **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 individual, 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 is 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.

17. **School records** refer to the records of students of all acts, events, accomplishments, results or research and all documents depicting the various activities of the students. This includes, but are not limited to, the following:
    1. Personal and academic records of the student
    2. Baptismal and Birth Certificates
    3. Academic reports
    4. Medical and Records
    5. Guidance and Disciplinary records
    6. Alien Certificate (for foreign students)
    7. Individual financial records (i.e. individual tuition fee payments, balances etc.)

18. **University personnel** means all employees (regardless of the type of employment or contractual arrangement) of the University.

IV. SCOPE AND LIMITATIONS

This Manual applies to all students and employees regardless of employment status, parents or guardians of minor students, third parties including applicants for admission or employment and former students or alumni whose school records are required to be kept and secured by the University. The data covered by this Manual is limited to personal information, as defined under Section III, collected and processed by the University.

V. COLLECTION OF PERSONAL INFORMATION

A. Privacy Principles

1. **TRANSPARENCY.** Data subject's consent should be obtained before collecting the information and the latter should be informed of the purpose for which the information is to be collected.

    Example:
    In the enrolment process, students are required to fill out the Student Information Sheet. The purpose of such collection of information is stated in the form and the consent of the student is obtained through the form filled out and signed by the student.

2. **PROPORTIONALITY.** Personal Information collected must be reasonably necessary or directly related to the University's functions.

    Example:
    In the application for admission as a college student in USM, only information such as name, address, contact numbers, previous schools, parent's or guardian's name, which are necessary for the evaluation of eligibility for admission to the University is collected.

3. **LEGIMATE PURPOSE.** In collecting personal information, the University shall use the information only for legitimate purposes as discussed in Section VI of this Manual

    Example:
    Personal information such as student's name, parents' name and addresses and contact numbers etc., shall be used only for purposes such as enrolment, academic activities and availment of student services which is allowed under the provisions of the USM Code.

B. **Provisions for Units in the University**

The access and release of personal data from the following offices shall be restricted to authorized persons as defined by their operation procedures:

1. The **University Admission and Records Office (ARO)** collects personal information for the purpose of determining eligibility of the applicant for admission or in the case of current students, for continuing enrollment in the University.
2. The **Human Resource Management and Development Office** (HRMDO)collects personal information from employees or applicants for purposes of evaluating the applicant for eligibility for employment, and availment of employee benefits (i.e. retirement, educational and medical benefits) and collates the information in the individual 201 files of the employees as required under the provisions of the Labor Code.

   Pursuant to existing labor laws and human resources policies of the University, the 201 files or employee's individual employment records are confidential and access is restricted to authorized personnel only.
3. The **University Hospital** collects sensitive information relating to the medical and dental health of students, faculty and staff for monitoring purposes. Access to the data collected is restricted and limited only to authorized personnel in the department such as the school doctor, dentist or nurse. Sensitive information may not be released without the prior consent of the student or guardian except in cases where the life of the student or other students (i.e. epidemic cases as provided under the DOH rules and regulations) is at stake.
4. The **University Guidance Center** (UGC) personal data for the purposes of individual inventory, counselling, academic follow-up, testing and other related guidance services.
5. The **University Information and Communication Technology Office** (UICTO) processes, secures and stores personal information in data base systems in the University. All personal information collected from students by the different units are primarily stored in the Student Information database. Employee personal information collected by the HRMDO is stored in the Human Resource Information database.

   Access to the data is restricted and given only to predetermined authorized personnel in relation to their specific function which requires access to process student or employee information. All access to personal information of students must be with their or their parents'/ guardians' consent, or employee's consent and must be for legitimate purposes, or endorsed by the Department head, and approved by the UICTO Head or his authorized representative.
6. The **Records Section** is tasked to ensure the systematic flow and monitoring of documents within the University and coming from outside the University. Communication which contain personal information shall be held confidential by the receiving and releasing officers.
7. **Other Units**

   All other units who collect, process or store student or employee personal information, if any, are subject to the policies provided under this Manual. Unit heads are responsible for ensuring compliance of the provisions of this Manual within their departments.

   The Data Privacy Act exempts the collection of personal data for research purposes. However, the University is still duty-bound to ensure that members of the USM community provide informed consent when they are asked to participate in any study. The Research Office of the University, through relevant units under it, shall ensure that this safeguard is in place.

C. **Privacy Policies**

To ensure that the rights of the data subjects are protected, the above-mentioned units are subject to the following policies:

1. **Notification of and securing consent from data subjects**

Collection of information is done with the consent of data subjects (employees, students and their guardians). Consent is indicated in the forms filled out during application for admission, enrollment or availment of student services such as scholarships, on the job trainings; and in the case of employees, promotion or re-classification, etc.

Forms for collection of personal information by different units in the University shall include a provision or a variation of these privacy statements:

> All information shall be used by the University for legitimate purposes, specifically for_____ and shall be processed by authorized personnel in accordance with the Data Privacy Policy of the University."
>
> "I hereby allow/authorize _____ to use, collect and process the information for legitimate purposes specifically for _____, and allow authorized personnel to process the information."

3. Policy on Access to Personal Information

Only authorized personnel are allowed to access and process the personal information collected from the students, their parents or guardians in accordance with Data Privacy policies of the University which requires that student records as well as the information contained therein are to be kept confidential.

Example: Only the registrar or her duly authorized representative or personnel is allowed complete access to the student profile which includes the name, student number, parents' names, addresses, contact numbers, grades etc.

3. **Policy on Collection of Personal Information**

Authorized university personnel shall collect personal information which is reasonably necessary or directly related to the University's primary or secondary functions or activities. Personal Information shall not be collected in anticipation that it may be useful in the future. The physical records or those which are not digitally stored and secured in the USM database are stored in particular offices of each Unit, access to which is controlled by the Unit Head.

For student records which are required to be perpetually stored and maintained by the University, an office is maintained to physically store and secure the records. Access is restricted where such records may only be retrieved upon specific instructions of the Unit Head and only for legitimate purposes or upon request of the student or alumni for copies of their individual school record or pursuant to the Unit's procedures and policies on request for records.

Personal information shall be collected by lawful and fair means, which is allowed under the University's policies and provided by the USM Code.

Example:

> For foreign students, nationality, ACR numbers, passport numbers and the contact numbers of the parents are guardians are necessary in case of emergencies and other situations where the student's parents or embassy are required to be notified.

VI. USE AND DISCLOSURE OF INFORMATION

Authorized university personnel are allowed to access, use and process said information for legitimate primary or secondary purposes of the University and/or that which is stated in the privacy statement contained in the forms or documents signed by the students or employees.

A. Primary Purpose

As a higher education institution, personal information is collected primarily for the educational purposes of students and employment-related purposes of employees. This includes monitoring academic activities as well as extracurricular activities of students, pursuant to the USM Code, and monitoring potential and current employees in accordance with labor laws. This also includes information collected for purposes set out in the privacy statements contained in the documents signed by students or employees. Such information is allowed to be processed and used by authorized personnel for such purposes.

B. Secondary Purposes

Secondary purposes are those which are collateral to the primary purposes and which are necessary to process the information. This include monitoring the current administrative or disciplinary standing (for student and employee discipline), financial condition (for scholarship purposes) or the health and psychological wellness of students and employees (health purposes). Authorized university personnel are allowed to use personal information collected and/or processed for such purposes provided the following circumstances are present:

1. the student or employee has consented to the use or disclosure for the secondary purpose; or;
2. the student or employee would reasonably expect the University, through its authorized personnel, to use, or process personal information for secondary purposes directly related to the primary purposes

C. Policy on Sensitive Personal Information

Sensitive personal information may not be disclosed or processed, except in any of the following cases:

1. Consent is given by data subject, prior to the processing of the sensitive personal information or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose of the University.
2. The processing of the sensitive personal information provided for by existing laws and regulations, such as medical history that need to be disclosed by the student as part of the monitoring of the health of the student, provided, that said laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data.
3. 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.
4. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations provided that the processing is confined and related to the bona fide members of these organizations or their associations; the sensitive personal information are not transferred to third parties; and consent of the data subject was obtained prior to processing.
5. The processing is necessary for the purpose of medical treatment; provided, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured.

6. The processing concerns sensitive personal information or privileged information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

D. Government-Related Use and Disclosure of Personal Information

Personal information is allowed to be used and disclosed to government agencies to satisfy reportorial requirements in line with their constitutionally or legislatively mandated functions pursuant to existing education or labor laws or when the use of pursuant to lawful order of a court or tribunal.

VII. ENSURING AND MAINTAINING ACCURACY OF INFORMATION

A. **Verification of information**

Authorized university personnel must take reasonable steps to ensure that the personal information collected or processed, up-to-date, complete, relevant and not misleading. The information collected from students and employees shall be verified by the units collecting the information.

Example:
Student information is verified by the Admission and Records Office while the HRD conducts the verification of employee information and background checks.

B. **Correction and updating of information**

Students and employees shall update their personal information through forms available at the Data Protection Office or in the Office holding their information. In case of erroneous or false information, data subjects may request correction, rectification, blocking or erasure (only to the extent allowed by the Data Privacy Act and other applicable laws) using the same process.

VIII. SECURITY OF PERSONAL INFORMATION

A. **Security Measures**

1. Technical Measures

The University shall take reasonable steps to protect the personal information in its possession from misuse, loss or unauthorized access, modification or disclosure. As most of the personal information of students and employees are stored in the University databases, access to personal information in digital or digitized form by authorized IT personnel is restricted and individually identifiable.

internal requests (i.e. special requests for authority to view student profile for disciplinary cases, counselling, or health concerns) for access to restricted student or employee records contained in the University information systems shall be sent through the President for approval before access is granted.

As a general rule only authorized personnel with the necessary approvals may request for access of the information systems of personal information in accordance with the procedure established by the DPO. Physical access to the servers and network equipment is highly restricted to authorized personnel only. Security devices are employed to safeguard the university network and its systems.

A 24-hour security system is also provided by the University to secure the areas where the University data centers are located.

3. Physical Measures

Access to student and employee personal information is limited to authorized personnel of the specific units collecting or processing the information. Aside from access restriction, storage facilities for hard copies of documents containing personal information are also secured (i.e. locked) in cabinets or storage facilities.

Only authorized personnel may open or have access to keys to the storage facilities. The storage units or facilities are placed in areas which are not usually accessible to the public, safe from physical hazards such as rain, wind and dust, and located in areas which are usually manned by the authorized personnel.

Round-the-clock security is also provided for the entire University including areas where the hard copies of such documents are kept and secured. Buildings equipped with closed-circuit television (CCTV) should bear the sign: *This building is equipped with a CCTV. Your activities will be recorded for security purposes only. Should we need the footages for other purposes, your consent will be secured.*

B. Request for Access

As a general rule, only authorized personnel shall have access to student or employee personal information. Students, employees, parents or guardians (in case of minors) who wish to have access to their own personal information may submit a written request directly to the Unit or Office and may be allowed access to their specific individual information or given copies, pursuant to the policies and guidelines on requesting for access or copies of student records. Request for information through telephone is not allowed. In case of email inquiries, proof of parent or student identity shall be submitted along with the email request.

Employees who wish to view the personal information in their individual personnel file may file a written request or directly go to the HRD Office, and request for viewing of such information in the presence of an authorized personnel of the department.

As a general rule, only authorized personnel may be allowed to have access to the personal information subject to the procedure established in this section. In such cases where any individual or entity [other than the student, parent or guardian in the case of minors, or employee] wishes to have access pursuant to the instances or exceptions provided under Data Privacy Act or Article VI of this Manual, a written request shall be submitted to the Unit Head who may either endorse or reject the same. If approved, the endorsed request shall be submitted to the DPO or the duly authorized representative for approval. If the request involves digital or digitized data, approval of the UICTO Director is required prior to endorsement of the Unit Head to the DPO. Only written requests properly endorsed by the Unit Head shall be considered for approval.

The written request shall state the name of the requestor, the purpose, the type of access requested (i.e. copying or viewing only), and the time frame or time limit within which access shall be given with a guarantee that the information shall be used solely for purposes allowed by law and a statement that such shall be treated with utmost confidentiality

In cases where government agencies empowered under the law to request for personal information (i.e., BIR, DOH), request for access, university personnel must ensure that the request is in writing and cities the authority or basis upon which the request is made. In cases where the request is a result of a valid order or decision of a tribunal or court, a copy of such order shall be attached to the written request.

Once approved by the DPO, it shall be transmitted to the Unit Head of the appropriate Unit for implementation. The Unit Head who endorsed the same shall be responsible for monitoring compliance of the requestor on the terms of the approved request (i.e., time limit and confidentiality).

In case there is doubt on the propriety of any request for access, university personnel should consult with or seek clearance from the DPO.

C. Retention and Destruction of Personal Information

Under the provisions of applicable laws, the University is required to permanently keep the student and employee records including the information contained therein. In line with this, no personal information may be destroyed unless allowed by such laws, and such destruction, if allowed or authorized by law and the University, must be documented in writing by the University. Unauthorized destruction should be reported to the DPO or any member of the Breach Incident Response Team pursuant to the procedure stated in the succeeding section.

IX. INQUIRY AND COMPLAINTS

A. Inquiry on Data Privacy matters and issues

Data subjects may request for information from the Data Protection Officer regarding any issue relating to the processing of their personal data under the custody of USM, including the data privacy and security policies implemented to ensure the protection of their personal data.

B. Procedure for Complaints

Any suspected or actual breach of the provisions of the USM Data Privacy Manual, violation of data privacy rights, or any breach, loss or unauthorized access or disclosure of personal information in the possession or under the custody of the University must be reported in writing immediately to the any member of the Breach Incident Response Team.

In case of a complaint for violation of the provisions USM Data Privacy policies, or any serious breach, loss or unauthorized access, disclosure or destruction of personal information in the possession or under the custody of the University, a report shall be made to the National Privacy Commission within seventy-two (72) hours from knowledge of the breach incident.

Within reasonable time, the DPO or any (2) members of the Breach Incident Response Team shall verify the allegations in the complaint. If warranted, an official investigation shall be conducted in cases of serious security breach as provided under Republic Act No. 10173. The results of the investigation shall be reported to the National Privacy Commission.

The DPO may also convene the entire team in case of a complaint, or motu-propio in case the violation of policies or data breach, loss, unauthorized access or destruction as an investigation committee to recommend actions, particularly when the violation is serious or causes or has the potential to cause material damage to the University or any of its students or employees. Such recommendation shall be submitted to the President of the University for approval.

Any appeal on such approved recommendation/Decision shall be made by any of the affected parties within 15 days from receipt of the approved Decision.

USM DATA PRIVACY TEAM:

1. **FRANCISCO GIL N. GARCIA, RPAE, Ph.D.**
   University President/Personal Information Controller
   op@usm.edu.ph

2. **JENNIFER E. SINCO**
   Data Protection Officer
   dpo@usm.edu.ph

X. EFFECTIVITY

The provisions of this Manual shall take effect on March 12, 2020.

XI. ANNEXES

A. IRR OF RA 10173 (DATA PRIVACY ACT OF 2012)
B. DATA PRIVACY NOTICE
C. CONSENT FORM
D. NONDISCLOSURE AGREEMENT FOR EMPLOYEES
E. DATA INQUIRY/ACCESS REQUEST FORM

ANNEX A: **IMPLEMENTING RULES AND REGULATIONS OF THE DATA PRIVACY ACT OF 2012 REPUBLIC OF THE PHILIPPINES**

Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012

Pursuant to the mandate of the National Privacy Commission to administer and implement the provisions of the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection, the following rules and regulations are hereby promulgated to effectively implement the provisions of the Act:

Rule I. Preliminary Provisions

1. Title
2. Policy
3. Definitions

Rule II. Scope of Application

4. Scope
5. Special Cases
6. Protection afforded to data subjects
7. Protection afforded to journalists and their sources

Rule III. National Privacy Commission

8. Mandate
9. Functions
10. Administrative Issuances
11. Reports and Public Information
12. Confidentiality of Personal Data
13. Organizational Structure
14. Secretariat
15. Effect of Lawful Performance of Duty
16. Magna Carta for Science and Technology Personnel

Rule IV. Data Privacy Principles

17. General Principles
18. Principles of Transparency, Legitimate Purpose and Proportionality
19. Principles in Collection, Processing and Retention

a. Collection must be for a specified and legitimate purpose
b. Personal Data shall be processed fairly and lawfully
c. Processing should ensure data quality
d. Personal data shall not be retained longer than necessary
e. Any authorized further processing shall have adequate safeguards

20. Principles for Data Sharing

Rule V. Lawful Processing of Personal Data

21. Lawful Processing of Personal Information
22. Lawful Processing of Sensitive Personal Information and Privileged Information
23. Extension of Privileged Communication
24. Surveillance of Subjects and Interception of Recording of Communications

Rule VI. Security Measures for Protection of Personal Data

25. Data Privacy and Security
26. Organizational Security
27. Physical Security
28. Technical Security
29. Appropriate Level of Security

Rule VII. Security of Sensitive Personal Information in Government
30. Responsibility of Heads of Agencies
31. Requirements Relating to Access by Agency Personnel to Sensitive Personal Information
32. Implementation of Security Requirements
33. Applicability to Government Contractors

Rule VIII. Rights of Data Subject
34. Rights of the Data Subject
a. Right to be informed
b. Right to object
c. Right to access
d. Right to correct
e. Right to rectification, erasure or blocking
35. Transmissibility of Rights of the Data Subject
36. Right to Data Portability
37. Limitation on Rights

Rule IX. Data Breach Notification
38. Data Breach Notification
39. Contents of Notification
40. Delay of Notification
41. Breach Report
42. Procedure for Notification

Rule X. Outsourcing and Subcontracting Agreements
43. Subcontract of Personal Data
44. Agreements for Outsourcing
45. Duty of Personal Information Processor

Rule XI. Registration and Compliance Requirements
46. Enforcement of the Data Privacy Act
47. Registration of Data Processing Systems
48. Notification for Automated Processing Operations
49. Review by the Commission

Rule XII. Rules on Accountability
50. Accountability for Transfer of Personal Information
51. Accountability for Violation of the Act, these Rules and other issuances

Rule XIII. Penalties
52. Unauthorized Processing of Personal Information and Sensitive Personal Information
53. Accessing Personal Information and Sensitive Personal Information Due to Negligence
54. Improper Disposal of Personal Information and Sensitive Personal Information
55. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes
56. Unauthorized Access or Intentional Breach
57.Concealment of Security Breaches Involving Sensitive Personal Information
58. Malicious Disclosure
59. Unauthorized Disclosure
60. Combination or Series of Acts
61. Extent of Liability
62. Large-Scale
63. Offense Committed by Public Officer
64. Restitution
65. Fines and Penalties

Rule XIV. Miscellaneous Provisions
66. Appeal
67. Period for Compliance
68. Appropriations Clause
69. Interpretation
70. Separability Clause
71. Repealing Clause
72. Effectivity Clause

Rule I. Preliminary Provisions

Section 1. Title. These rules and regulations shall be known as the "Implementing Rules and Regulations of the Data Privacy Act of 2012", or the "Rules".

Section 2. Policy. These Rules further enforce the Data Privacy Act and adopt generally accepted international principles and standards for personal data protection. They safeguard the fundamental human right of every individual to privacy while ensuring free flow of information for innovation, growth, and national development. These Rules also recognize the vital role of information and communications technology in nation-building and enforce the State's inherent obligation to ensure that personal data in information and communications systems in the government and in the private sector are secured and protected.

Section 3. Definitions. Whenever used in these Rules, the following terms shall have the respective meanings hereafter set forth:
a. "Act" refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012;
b. "Commission" refers to the National Privacy Commission.
c. "Consent of the data subject" refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so;
d. "Data subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;
e. "Data processing systems" refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;
f. "Data sharing" is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor;
g. "Direct marketing" refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals;
h. "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
i. "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 which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document;
j. "Personal data" refers to all types of personal information;
k. "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;

l. "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;
m. "Personal information controller" refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:
1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;
There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;
n. "Personal information processor" refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;
o. "Processing" refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system;
p. "Profiling" refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
q. "Privileged information" refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication;
r. "Public authority" refers to any government entity created by the Constitution or law, and vested with law enforcement or regulatory authority and functions;
s. "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 would result to a personal data breach, if not for safeguards that have been put in place;
t. 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 offense committed or alleged to have been committed by such individual, 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 is 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.

Rule II. Scope of Application

Section 4. Scope. The Act and these Rules apply to the processing of personal data by any natural and juridical person in the government or private sector. They apply to an act done or practice engaged in and outside of the Philippines if:
a. The natural or juridical person involved in the processing of personal data is found or established in the Philippines;
b. The act, practice or processing relates to personal data about a Philippine citizen or Philippine resident;
c. The processing of personal data is being done in the Philippines; or

d. The act, practice or processing of personal data is done or engaged in by an entity with links to the Philippines, with due consideration to international law and comity, such as, but not limited to, the following:
1. Use of equipment located in the country, or maintains an office, branch or agency in the Philippines for processing of personal data;
2. A contract is entered in the Philippines;
3. A juridical entity unincorporated in the Philippines but has central management and control in the country;
4. An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal data;
5. An entity that carries on business in the Philippines;
6. An entity that collects or holds personal data in the Philippines.

Section 5. Special Cases. The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:

a. Information processed for purpose of allowing public access to information that fall within matters of public concern, pertaining to:
1. Information about any individual who is or was an officer or employee of government that relates to his or her position or functions, including:
(a) The fact that the individual is or was an officer or employee of the government; The title, office address, and office telephone number of the individual;
(b) The classification, salary range, and responsibilities of the position held by the individual;
(c) The name of the individual on a document he or she prepared in the course of his or her employment with the government; and;

2. Information about an individual who is or was performing a service under contract for a government institution, but only in so far as it relates to such service, including the name of the individual and the terms of his or her contract;
3. Information relating to a benefit of a financial nature conferred on an individual upon the discretion of the government, such as the granting of a license or permit, including the name of the individual and the exact nature of the benefit: Provided, that they do not include benefits given in the course of an ordinary transaction or as a matter of right;

b. Personal information processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations;

c. Personal information that will be processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards;

d. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law. Nothing in this Act shall be construed as having 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);

e. Information necessary for banks, other financial institutions under the jurisdiction of the independent, central monetary authority or Bangkok Sentral ng Pilipinas, and other bodies authorized by law, to the extent necessary to comply with Republic Act No. 9510 (CISA), Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act, and other applicable laws;

f. 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. The burden of proving the law of the foreign jurisdiction falls on the person or body seeking exemption. In the absence of proof, the applicable law shall be presumed to be the Act and these Rules: Provided, that the non-applicability of the Act or these Rules do not extend to personal information controllers or personal information processors, who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity.

Section 6. Protection afforded to Data Subjects

a. Unless directly incompatible or inconsistent with the preceding sections in relation to the purpose, function, or activities the non-applicability concerns, the personal information controller or personal information processor shall uphold the rights of data subjects, and adhere to general data privacy principles and the requirements of lawful processing.
b. The burden of proving that the Act and these Rules are not applicable to a particular information falls on those involved in the processing of personal data or the party claiming the non-applicability.
c. In all cases, the determination of any exemption shall be liberally interpreted in favor of the rights and interests of the data subject.

Section 7. Protection Afforded to Journalists and their Sources.

a. Publishers, editors, or duly accredited reporters of any newspaper, magazine or periodical of general circulation shall not be compelled to reveal the source of any news report or information appearing in said publication if it was related in any confidence to such publisher, editor, or reporter.
b. Publishers, editors, or duly accredited reporters who are likewise personal information controllers or personal information processors within the meaning of the law are still bound to follow the Data Privacy Act and related issuances with regard to the processing of personal data, upholding rights of their data subjects and maintaining compliance with other provisions that are not incompatible with the protection provided by Republic Act No. 53.

Rule III. National Privacy Commission

Section 8. Mandate. The National Privacy Commission is an independent body mandated to administer and implement the Act, and to monitor and ensure compliance of the country with international standards set for personal data protection.

Section 9. Functions. The National Privacy Commission shall have the following functions:

a. Rule Making. The Commission shall develop, promulgate, review or amend rules and regulations for the effective implementation of the Act. This includes:

1. Recommending organizational, physical and technical security measures for personal data protection, encryption, and access to sensitive personal information maintained by government agencies, considering the most appropriate standard recognized by the information and communications technology industry, as may be necessary;
2. Specifying electronic format and technical standards, modalities and procedures for data portability, as may be necessary;
3. Issuing guidelines for organizational, physical, and technical security measures for personal data protection, taking into account the nature of the personal data to be protected, the risks presented by the processing, the size of the organization and complexity of its

operations, current data privacy best practices, cost of security implementation, and the most appropriate standard recognized by the information and communications technology industry, as may be necessary;

4. Consulting with relevant regulatory agencies in the formulation, review, amendment, and administration of privacy codes, applying the standards set out in the Act, with respect to the persons, entities, business activities, and business sectors that said regulatory bodies are authorized to principally regulate pursuant to law;

5. Proposing legislation, amendments or modifications to Philippine laws on privacy or data protection, as may be necessary;

6. Ensuring proper and effective coordination with data privacy regulators in other countries and private accountability agents;

7. Participating in international and regional initiatives for data privacy protection.

b. Advisory. The Commission shall be the advisory body on matters affecting protection of personal data. This includes:

1. Commenting on the implication on data privacy of proposed national or local statutes, regulations or procedures, issuing advisory opinions, and interpreting the provisions of the Act and other data privacy laws;

2. Reviewing, approving, rejecting, or requiring modification of privacy codes voluntarily adhered to by personal information controllers, which may include private dispute resolution mechanisms for complaints against any participating personal information controller, and which adhere to the underlying data privacy principles embodied in the Act and these Rules;

3. Providing assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person, including the enforcement of rights of data subjects;

4. Assisting Philippine companies doing business abroad to respond to data protection laws and regulations.

c. Public Education. The Commission shall undertake necessary or appropriate efforts to inform and educate the public of data privacy, data protection, and fair information rights and responsibilities. This includes:

1. Publishing, on a regular basis, a guide to all laws relating to data protection;

2. Publishing a compilation of agency system of records and notices, including index and other finding aids;

3. Coordinating with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal data in the country;

d. Compliance and Monitoring. The Commission shall perform compliance and monitoring functions to ensure effective implementation of the Act, these Rules, and other issuances.
This includes:

1. Ensuring compliance by personal information controllers with the provisions of the Act;

2. Monitoring the compliance of all government agencies or instrumentalities as regards their security and technical measures, and recommending the necessary action in order to meet minimum standards for protection of personal data pursuant to the Act;

3. Negotiating and contracting with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

4. Generally performing such acts as may be necessary to facilitate cross-border enforcement of data privacy protection;

5. Managing the registration of personal data processing systems in the country, including the personal data processing system of contractors and their employees entering into contracts with government agencies that involves accessing or requiring sensitive personal information of at least one thousand (1,000) individuals.

e. Complaints and Investigations. The Commission shall adjudicate on complaints and investigations on matters affecting personal data: Provided, that in resolving any complaint or investigation, except where amicable settlement is reached by the parties, the Commission shall act as a collegial body. This includes:

1. Receiving complaints and instituting investigations regarding violations of the Act, these Rules, and other issuances of the Commission, including violations of the rights of data subjects and other matters affecting personal data;
2. Summoning witnesses, and requiring the production of evidence by a subpoena duces for the purpose of collecting the information necessary to perform its functions under the Act: Provided, that the Commission may be given access to personal data that is subject of any complaint;
3. Facilitating or enabling settlement of complaints through the use of alternative dispute resolution processes, and adjudicating on matters affecting any personal data;
4. Preparing reports on the disposition of complaints and the resolution of any investigation it initiates, and, in cases it deems appropriate, publicizing such reports;

f. Enforcement. The Commission shall perform all acts as may be necessary to effectively implement the Act, these Rules, and its other issuances, and to enforce its Orders, Resolutions or Decisions, including the imposition of administrative sanctions, fines, or penalties. This includes:
1. Issuing compliance or enforcement orders;
2. Issuing compliance or enforcement orders;
3. Issuing cease and desist orders, or imposing a temporary or permanent ban on the processing of personal data, upon finding that the processing will be detrimental to national security or public interest, or if it is necessary to preserve and protect the rights of data subjects;
4. Recommending to the Department of Justice (DOJ) the prosecution of crimes and imposition of penalties specified in the Act;
5. Compelling or petitioning any entity, government agency, or instrumentality, to abide by its orders or take action on a matter affecting data privacy;
6. Imposing administrative fines for violations of the Act, these Rules, and other issuances of the Commission.

g. Other functions. The Commission shall exercise such other functions as may be necessary to fulfill its mandate under the Act.

Section 10. Administrative Issuances. The Commission shall publish or issue official directives and administrative issuances, orders, and circulars, which include:
a. Rules of procedure in the exercise of its quasi-judicial functions, subject to the suppletory application of the Rules of Court;
b. Schedule of administrative fines and penalties for violations of the Act, these Rules, and issuances or Orders of the Commission, including the applicable fees for its administrative services and filing fees;
c. Procedure for registration of data processing systems, and notification;
d. Other administrative issuances consistent with its mandate and other functions.

Section 11. Reports and Information. The Commission shall report annually to the President and Congress regarding its activities in carrying out the provisions of the Act, these Rules, and its other issuances. It shall undertake all efforts it deems necessary or appropriate to inform and educate the public of data privacy, data protection, and fair information rights and responsibilities.

Section 12. Confidentiality of Personal Data. Members, employees, and consultants of the Commission shall ensure at all times the confidentiality of any personal data that come to their

knowledge and possession: Provided, that such duty of confidentiality shall remain even after their term, employment, or contract has ended.

Section 13. Organizational Structure. The Commission is attached to the Department of Information and Communications Technology for policy and program coordination in accordance with Section 38(3) of Executive Order No. 292, series of 1987, also known as the Administrative Code of 1987. The Commission shall remain completely independent in the performance of its functions. The Commission shall be headed by a Privacy Commissioner, who shall act as Chairman of the Commission. The Privacy Commissioner must be at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, and a recognized expert in the field of information technology and data privacy. The Privacy Commissioner shall enjoy the benefits, privileges, and emoluments equivalent to the rank of Secretary. The Privacy Commissioner shall be assisted by two (2) Deputy Privacy Commissioners. One shall be responsible for Data Processing Systems, while the other shall be responsible for Policies and Planning. The Deputy Privacy Commissioners must be recognized experts in the field of information and communications technology and data privacy. They shall enjoy the benefits, privileges, and emoluments equivalent to the rank of Undersecretary.

Section 14. Secretariat. The Commission is authorized to establish a Secretariat, which shall assist in the performance of its functions. The Secretariat shall be headed by an Executive Director and shall be organized according to the following offices:

a. Data Security and Compliance Office;
b. Legal and Enforcement Office;
c. Finance and Administrative Office;
d. Privacy Policy Office;
e. Public Information and Assistance Office.

Majority of the members of the Secretariat, in so far as practicable, must have served for at least five (5) years in any agency of the government that is involved in the processing of personal data including, but not limited to, the following offices: Social Security System (SSS), Government Service Insurance System (GSIS), Land Transportation Office (LTO), Bureau of Internal Revenue (BIR), Philippine Health Insurance Corporation (PhilHealth), Commission on Elections (COMELEC), Department of Foreign Affairs (DFA), Department of Justice (DOJ), and Philippine Postal Corporation (Philpost).

The organizational structure shall be subject to review and modification by the Commission, including the creation of new divisions and units it may deem necessary, and shall appoint officers and employees of the Commission in accordance with civil service law, rules, and regulations.

Section 15. Effect of Lawful Performance of Duty. The Privacy Commissioner, the Deputy Commissioners, or any person acting on their behalf or under their direction, shall not be civilly liable for acts done in good faith in the performance of their duties: Provided, that they shall be liable for willful or negligent acts, which are contrary to law, morals, public policy, and good customs, even if they acted under orders or instructions of superiors: Provided further, that in case a lawsuit is filed against them in relation to the performance of their duties, where such performance is lawful, he or she shall be reimbursed by the Commission for reasonable costs of litigation.

Section 16. Magna Carta for Science and Technology Personnel. Qualified employees of the Commission shall be covered by Republic Act No. 8349, which provides a magna carta for scientists, engineers, researchers, and other science and technology personnel in the government.

Rule IV. Data Privacy Principles

Section 17. General Data Privacy Principles. The processing of personal data shall be allowed, subject to compliance with the requirements of the Act and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose, and proportionality.

Section 18. Principles of Transparency, Legitimate Purpose and Proportionality.
The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.

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

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.

Section 19. General principles in collection, processing and retention. The processing of personal data shall adhere to the following general principles in the collection, processing, and retention of personal data:
a. Collection must be for a declared, specified, and legitimate purpose.
1. Consent is required prior to the collection and processing of personal data, subject to exemptions provided by the Act and other applicable laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn.
2. The data subject must be provided specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his or her personal data for profiling, or processing for direct marketing, and data sharing.
3. Purpose should be determined and declared before, or as soon as reasonably practicable, after collection.
4. Only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected.

b. Personal data shall be processed fairly and lawfully.
1. Processing shall uphold the rights of the data subject, including the right to refuse, withdraw consent, or object. It shall likewise be transparent, and allow the data subject sufficient information to know the nature and extent of processing.
2. Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.
3. Processing must be in a manner compatible with declared, specified, and legitimate purpose.
4. Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
5. Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.

c. Processing should ensure data quality.

1. Personal data should be accurate and where necessary for declared, specified and legitimate purpose, kept up to date.
2. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

d. Personal Data shall not be retained longer than necessary.
1. Retention of personal data shall only be for as long as necessary:
(a) for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
(b) for the establishment, exercise or defense of legal claims; or
(c) for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.
2. Retention of personal data shall be allowed in cases provided by law.
3. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.

e. Any authorized further processing shall have adequate safeguards.
1. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organizational, physical, and technical security measures required by the Act in order to safeguard the rights and freedoms of the data subject.
2. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.
3. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

Section 20. General Principles for Data Sharing. Further Processing of Personal Data collected from a party other than the Data Subject shall be allowed under any of the following conditions:

a. Data sharing shall be allowed when it is expressly authorized by law: Provided, that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose and proportionality.

b. Data Sharing shall be allowed in the private sector if the data subject consents to data sharing, and the following conditions are complied with:
1. Consent for data sharing shall be required even when the data is to be shared with an affiliate or mother company, or similar relationships;
2. Data sharing for commercial purposes, including direct marketing, shall be covered by a data sharing agreement.
(a) The data sharing agreement shall establish adequate safeguards for data privacy and security, and uphold rights of data subjects.
(b) The data sharing agreement shall be subject to review by the Commission, on its own initiative or upon complaint of data subject;

3. The data subject shall be provided with the following information prior to collection or before data is shared:
(a) Identity of the personal information controllers or personal information processors that will be given access to the personal data;
(b) the Purpose of data sharing;
(c) Categories of personal data concerned;
(d) Intended recipients or categories of recipients of the personal data;
(e) Existence of the rights of data subjects, including the right to access and correction, and right to object;
(f) Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

4. Further processing of shared data shall adhere to the data privacy principles laid down in the Act, these Rules, and other issuances of the Commission.

c. Data collected from parties other than the data subject for purpose of research shall be allowed when the personal data is publicly available, or has the consent of the data subject for purpose of research: Provided, that adequate safeguards are in place, and no decision directly affecting the data subject shall be made on the basis of the data collected or processed. The rights of the data subject shall be upheld without compromising research integrity.

d. Data sharing between government agencies for the purpose of a public function or provision of a public service shall be covered a data sharing agreement.
1. Any or all government agencies party to the agreement shall comply with the Act, these Rules, and all other issuances of the Commission, including putting in place adequate safeguards for data privacy and security.
2. The data sharing agreement shall be subject to review of the Commission, on its own initiative or upon complaint of data subject.

Rule V. Lawful Processing of Personal Data

Section 21. Criteria for Lawful Processing of Personal Information. Processing of personal information is allowed, unless prohibited by law. For processing to be lawful, any of the following conditions must be complied with:
a. The data subject must have given his or her consent prior to the collection, or as soon as practicable and reasonable;
b. The processing involves the personal information of a data subject who is a party to a contractual agreement, in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to entering the said agreement;
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 his or her life and health;
e. The processing of personal information is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law;
f. The processing of personal information is necessary for the fulfillment of the constitutional or statutory mandate of a public authority; or
g. The processing is necessary to pursue the legitimate interests of the personal information controller, or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject, which require protection under the Philippine Constitution.

Section 22. Sensitive Personal Information and Privileged Information. The processing of sensitive personal and privileged information is prohibited, except in any of the following cases:
a. Consent is given by data subject, or by the parties to the exchange of privileged information, prior to the processing of the sensitive personal information or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose;
b. The processing of the sensitive personal information or privileged information is provided for by existing laws and regulations: Provided, that said laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data;
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:

1. Processing is confined and related to the bona fide members of these organizations or their associations;
2. The sensitive personal information is not transferred to third parties; and
3. Consent of the data subject was obtained prior to processing;

e. The processing is necessary for the purpose of medical treatment: Provided, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured; or
f. The processing concerns sensitive personal information or privileged information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

Section 23. Extension of Privileged Communication. Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered from privileged information is inadmissible.

When the Commission inquires upon communication claimed to be privileged, the personal information controller concerned shall prove the nature of the communication in an executive session. Should the communication be determined as privileged, it shall be excluded from evidence, and the contents thereof shall not form part of the records of the case: Provided, that where the privileged communication itself is the subject of a breach, or a privacy concern or investigation, it may be disclosed to the Commission but only to the extent necessary for the purpose of investigation, without including the contents thereof in the records.

Section 24. Surveillance of Suspects and Interception of Recording of Communications.
Section 7 of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", is hereby amended to include the condition that the processing of personal data for the purpose of surveillance, interception, or recording of communications shall comply with the Data Privacy Act, including adherence to the principles of transparency, proportionality, and legitimate purpose.

Rule VI. Security Measures for the Protection of Personal Data

Section 25. Data Privacy and Security. Personal information controllers and personal information processors shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data.

The personal information controller and personal information processor shall take steps to ensure that any natural person acting under their authority and who has access to personal data, does not process them except upon their instructions, or as required by law.

The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing. These measures shall be implemented to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

Section 26. Organizational Security Measures. Where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for organizational security:

a. Compliance Officers. Any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall function as data protection officer, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security.

b. Data Protection Policies. Any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection policies that provide for organization, physical, and technical security measures, and, for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects.

1. The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.
2. The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility.
3. The polices shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices.

c. Records of Processing Activities. Any natural or juridical person or other body involved in the processing of personal data shall maintain records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data. Records should include:

1. Information about the purpose of the processing of personal data, including any intended future processing or data sharing;
2. A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing;
3. General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data;
4. A general description of the organizational, physical, and technical security measures in place;
5. The name and contact details of the personal information controller and, where applicable, the joint controller, the its representative, and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

d. Management of Human Resources. Any natural or juridical person or other entity involved in the processing of personal data shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data.

The said employees, agents, or representatives shall operate and hold personal data under strict confidentiality if the personal data are 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.

e. Processing of Personal Data. Any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review:

1. A procedure for the collection of personal data, including procedures for obtaining consent, when applicable;
2. Procedures that limit the processing of data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose;
3. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems;
4. Policies and procedures for data subjects to exercise their rights under the Act;
5. Data retention schedule, including timeline or conditions for erasure or disposal of records.

f. Contracts with Personal Information Processors. The personal information controller, through appropriate contractual agreements, shall ensure that its personal information processors, where applicable, shall also implement the security measures required by the Act

and these Rules. It shall only engage those personal information processors that provide sufficient guarantees to implement appropriate security measures specified in the Act and these Rules, and ensure the protection of the rights of the data subject.

Section 27. Physical Security Measures. Where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for physical security:

a. Policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media;

b. Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public;

c. The duties, responsibilities and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time;

d. Any natural or juridical person or other body involved in the processing of personal data shall implement Policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of personal data;

e. Policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

Section 28. Guidelines for Technical Security Measures. Where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures:

a. A security policy with respect to the processing of personal data;

b. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;

c. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

d. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach;

e. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

f. A process for regularly testing, assessing, and evaluating the effectiveness of security measures;

g. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

Section 29. Appropriate Level of Security. The Commission shall monitor the compliance of natural or juridical person or other body involved in the processing of personal data, specifically their security measures, with the guidelines provided in these Rules and subsequent issuances of the Commission. In determining the level of security appropriate for a particular personal information controller or personal information processor, the Commission shall take into account the nature of the personal data that requires protection, the risks posed by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation. The security measures provided herein shall be subject to regular review and evaluation, and may be updated as necessary by the Commission in separate issuances, taking into account the most appropriate standard recognized by the information and communications technology industry and data privacy best practices.

Rule VII. Security of Sensitive Personal Information in Government

Section 30. Responsibility of Heads of Agencies. All sensitive personal information maintained by the government, its agencies, and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, subject to these Rules and other issuances of the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein. The Commission shall monitor government agency compliance and may recommend the necessary action in order to satisfy the minimum standards.

Section 31. Requirements Relating to Access by Agency Personnel to Sensitive Personal Information.

a. On-site and Online Access.

1. No employee of the government shall have access to sensitive personal information on government property or through online facilities unless he or she the employee has received a security clearance from the head of the source agency. The source agency is the government agency who originally collected the personal data.

2. A source agency shall strictly regulate access to sensitive personal information under its custody or control, particularly when it allows online access. An employee of the government shall only be granted a security clearance when the performance of his or her official functions or the provision of a public service directly depends on and cannot otherwise be performed unless access to the personal data is allowed.

3. Where allowed under the next preceding sections, online access to sensitive personal information shall be subject to the following conditions:

(a) An information technology governance framework has been designed and implemented;

(b) Sufficient organizational, physical and technical security measures have been established;

(c) The agency is capable of protecting sensitive personal information in accordance with data privacy practices and standards recognized by the information and communication technology industry;

(d) The employee of the government is only given online access to sensitive personal information necessary for the performance of official functions or the provision of a public service.

b. Off-site access.

1. Sensitive personal information maintained by an agency may not be transported or accessed from a location off or outside of government property, whether by its agent or employee, unless the head of agency has ensured the implementation of privacy policies and appropriate security measures. A request for such transportation or access shall be submitted to and approved by the head of agency. The request must include proper accountability mechanisms in the processing of data.

2. The head of agency shall approve requests for off-site access in accordance with the following guidelines:

(a) Deadline for Approval or Disapproval. The head of agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. Where no action is taken by the head of agency, the request is considered disapproved;

(b) Limitation to One thousand (1,000) Records. Where a request is approved, the head of agency shall limit the access to not more than one thousand (1,000) records at a time, subject to the next succeeding paragraph.

(c) 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 Commission.

Section 32. Implementation of Security Requirements. Notwithstanding the effective date of these Rules, the requirements in the preceding sections shall be implemented before any off-site or online access request is approved. Any data sharing agreement between a source agency and another government agency shall be subject to review of the Commission on its own initiative or upon complaint of data subject.

Section 33. Applicability to Government Contractors. In entering into any contract with a private service provider that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, a government agency shall require such service provider and its employees to register their personal data processing system with the Commission in accordance with the Act and these Rules. The service provider, as personal information processor, shall comply with the other provisions of the Act and these Rules, particularly the immediately preceding sections, similar to a government agency and its employees.

Rule VIII. Rights of Data Subjects

Section 34. Rights of the Data Subject. The data subject is entitled to the following rights:

a. Right to be informed.

1. The data subject has a right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.
2. The data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity:
(a) Description of the personal data to be entered into the system;
(b) Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
(c) Basis of processing, when processing is not based on the consent of the data subject;
(d) Scope and method of the personal data processing;
(e) The recipients or classes of recipients to whom the personal data are or may be disclosed;
(f) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
(g) The identity and contact details of the personal data controller or its representative;
(h) The period for which the information will be stored; and
(i) The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.

b. Right to object. The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph.

When a data subject objects or withholds consent, the personal information controller shall no longer process the personal data, unless:
1. The personal data is needed pursuant to a subpoena;
2. 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 to which the data subject is a party,

or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or

3. The information is being collected and processed as a result of a legal obligation.

c. Right to Access. The data subject has the right to reasonable access to, upon demand, the following:

1. Contents of his or her personal data that were processed;
2. Sources from which personal data were obtained;
3. Names and addresses of recipients of the personal data;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal data to recipients, if any;
6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
7. Date when his or her personal data concerning the data subject were last accessed and modified; and
8. The designation, name or identity, and address of the personal information controller.

d. Right to rectification. The data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: Provided, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.

e. Right to Erasure or Blocking. The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.

1. This right may be exercised upon discovery and substantial proof of any of the following:

(a) The personal data is incomplete, outdated, false, or unlawfully obtained;
(b) The personal data is being used for purpose not authorized by the data subject;
(c) The personal data is no longer necessary for the purposes for which they were collected;
(d) The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
(e) The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
(f) The processing is unlawful;
(g) The personal information controller or personal information processor violated the rights of the data subject.

2. The personal information controller may notify third parties who have previously received such processed personal information.

f. Right to damages. The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as data subject.

Section 35. Transmissibility of Rights of the Data Subject. The lawful heirs and assigns of the data subject may invoke the rights of the data subject to which he or she is an heir or an assignee, at any time after the death of the data subject, or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

Section 36. Right to Data Portability. Where his or her personal data is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the personal information controller a copy of such data in an electronic or structured

format that is commonly used and allows for further use by the data subject. The exercise of this right shall primarily take into account the right of data subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

Section 37. Limitation on Rights. The immediately preceding sections shall not be applicable if the processed personal data are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: Provided, that the personal data shall be held under strict confidentiality and shall be used only for the declared purpose. The said sections are also not applicable to the processing of personal data gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject. Any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research or investigation.

Rule IX. Data Breach Notification

Section 38. Data Breach Notification.

a. The Commission and affected data subjects shall be notified by the personal information controller within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the personal information controller or personal information processor that, a personal data breach requiring notification has occurred.
b. Notification of personal data breach shall be required when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.
c. Depending on the nature of the incident, or if there is delay or failure to notify, the Commission may investigate the circumstances surrounding the personal data breach. Investigations may include on-site examination of systems and procedures.

Section 39. Contents of Notification. The notification shall at least describe the nature of the breach, the personal data possibly involved, and the measures taken by the entity to address the breach. The notification shall also include measures taken to reduce the harm or negative consequences of the breach, the representatives of the personal information controller, including their contact details, from whom the data subject can obtain additional information about the breach, and any assistance to be provided to the affected data subjects.

Section 40. Delay of Notification. Notification may be delayed only 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.
a. In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal data.
b. The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest, or in the interest of the affected data subjects.
c. The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Section 41. Breach Report.

a. The personal information controller shall notify the Commission by submitting a report, whether written or electronic, containing the required contents of notification. The

report shall also include the name of a designated representative of the personal information controller, and his or her contact details.

b. All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of personal data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the personal information controller. In other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the Commission. A general summary of the reports shall be submitted to the Commission annually.

Section 42. Procedure for Notification. The Procedure for breach notification shall be in accordance with the Act, these Rules, and any other issuance of the Commission.

Rule X. Outsourcing and Subcontracting Agreements

Section 43. Subcontract of Personal Data. A personal information controller may subcontract or outsource the processing of personal data: Provided, that the personal information controller shall use contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the Act, these Rules, other applicable laws for processing of personal data, and other issuances of the Commission.

Section 44. Agreements for Outsourcing. Processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller.

a. 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 personal information controller, and the geographic location of the processing under the subcontracting agreement.

b. The contract or other legal act shall stipulate, in particular, that the personal information processor shall:

1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;
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 Act, these Rules, and other issuances of the Commission;
4. Not engage another processor without prior instruction from the personal information controller: 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 personal information controller, by appropriate technical and organizational 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 personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor;
7. At the choice of the personal information controller, delete or return all personal data to the personal information controller 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 Act or another law;
8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute

to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter;
9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission.

Section 45. Duty of personal information processor. The personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller.

Rule XI. Registration and Compliance Requirements

Section 46. Enforcement of the Data Privacy Act. Pursuant to the mandate of the Commission to administer and implement the Act, and to ensure the compliance of personal information controllers with its obligations under the law, the Commission requires the following:
a. Registration of personal data processing systems operating in the country that involves accessing or requiring sensitive personal information of at least one thousand (1,000) individuals, including the personal data processing system of contractors, and their personnel, entering into contracts with government agencies;
b. Notification of automated processing operations where the processing becomes the sole basis of making decisions that would significantly affect the data subject;

c. Annual report of the summary of documented security incidents and personal data breaches;
d. Compliance with other requirements that may be provided in other issuances of the Commission.

Section 47. Registration of Personal Data Processing Systems. The personal information controller or personal information processor that employs fewer than two hundred fifty (250) persons shall not be required to register unless the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal information of at least one thousand (1,000) individuals.

a. The contents of registration shall include:
1. The name and address of the personal information controller or personal information processor, and of its representative, if any, including their contact details;
2. The purpose or purposes of the processing, and whether processing is being done under an outsourcing or subcontracting agreement;
3. A description of the category or categories of data subjects, and of the data or categories of data relating to them;
4. The recipients or categories of recipients to whom the data might be disclosed;
5. Proposed transfers of personal data outside the Philippines;
6. A general description of privacy and security measures for data protection;
7.Brief description of the data processing system;
8. Copy of all policies relating to data governance, data privacy, and information security;
9. Attestation to all certifications attained that are related to information and communications processing; and
10. Name and contact details of the compliance or data protection officer, which shall immediately be updated in case of changes.

b. The procedure for registration shall be in accordance with these Rules and other issuances of the Commission.

Section 48. Notification of Automated Processing Operations. The personal information controller carrying out any wholly or partly automated processing operations or set of such operations intended to serve a single purpose or several related purposes shall notify the Commission when the automated processing becomes the sole basis for making decisions about a data subject, and when the decision would significantly affect the data subject.

a. The notification shall include the following information:
1. Purpose of processing;
2. Categories of personal data to undergo processing;
3. Category or categories of data subject;
4. Consent forms or manner of obtaining consent;
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 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.

Section 49. Review by the Commission. The following are subject to the review of the Commission, upon its own initiative or upon the filing of a complaint by a data subject:
a. Compliance by a personal information controller or personal information processor with the Act, these Rules, and other issuances of the Commission;
b. Compliance by a personal information controller or personal information processor with the requirement of establishing adequate safeguards for data privacy and security;
c. Any data sharing agreement, outsourcing contract, and similar contracts involving the processing of personal data, and its implementation;
d. Any off-site or online access to sensitive personal data in government allowed by a head of
agency;
e. Processing of personal data for research purposes, public functions, or commercial activities;
f. Any reported violation of the rights and freedoms of data subjects;
g. Other matters necessary to ensure the effective implementation and administration of the Act, these Rules, and other issuances of the Commission.

Rule XII. Rules on Accountability

Section 50. Accountability for Transfer of Personal Data. A personal information controller shall be responsible for any personal data under its control or custody, including information that have been outsourced or transferred to a personal information processor or a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

a. A personal information controller shall be accountable for complying with of the Act, these Rules, and other issuances of the Commission. It shall use contractual or other reasonable means to provide a comparable level of protection to the personal data while it is being processed by a personal information processor or third party.
b. A personal information controller shall designate an individual or individuals who are accountable for its compliance with the Act. The identity of the individual or individuals so designated shall be made known to a data subject upon request.

Section 51. Accountability for Violation of the Act, these Rules and Other Issuances of the Commission.

a. Any natural or juridical person, or other body involved in the processing of personal data, who fails to comply with the Act, these Rules, and other issuances of the Commission, 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.
b. In cases where a data subject files a complaint for violation of his or her rights as data subject, and for any injury suffered as a result of the processing of his or her personal data, the Commission may award indemnity on the basis of the applicable provisions of the New Civil Code.

c. 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 Commission 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 Commission based on substantial evidence.

Rule XIII. Penalties

Section 52. Unauthorized Processing of Personal Information and Sensitive Personal Information.

a. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under the Act or any existing law.
b. A penalty of imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process sensitive personal information without the consent of the data subject, or without being authorized under the Act or any existing law.

Section 53. Accessing Personal Information and Sensitive Personal Information Due to Negligence.

a. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under the Act or any existing law.
b. A penalty of imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to sensitive personal information without being authorized under the Act or any existing law.

Section 54. Improper Disposal of Personal Information and Sensitive Personal Information.
a. A penalty of imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) 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. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the sensitive personal information of an individual in an area accessible to the public or has otherwise placed the sensitive personal information of an individual in its container for trash collection.

Section 55. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.

a. A penalty of 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 (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under the Act or under existing laws.

b. A penalty of imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under the Act or under existing laws.

Section 56. Unauthorized Access or Intentional Breach. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) 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 are stored.

Section 57. Concealment of Security Breaches Involving Sensitive Personal Information. A penalty of 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 (Php500,000.00) but not more than One million pesos (Php1,000,000.00) 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) of the Act, intentionally or by omission conceals the fact of such security breach.

Section 58. 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 sensitive personal information obtained by him or her, shall be subject to 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 (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

Section 59. 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 (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

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 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

Section 60. Combination or Series of Acts. Any combination or series of acts as defined in Sections 52 to 59 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 (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

Section 61. Extent of Liability. If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. Where

applicable, the court may also suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and he or she is found guilty of acts penalized under Sections 54 and 55 of these Rules, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

Section 62. Large-Scale. The maximum penalty in the corresponding scale of penalties provided for the preceding offenses shall be imposed when the personal data of at least one hundred (100) persons are harmed, affected, or involved, as the result of any of the above-mentioned offenses.

Section 63. Offense Committed by Public Officer. When the offender or the person responsible for the offense is a public officer, as defined in the Administrative Code of 1987, in the exercise of his or her duties, he or she shall likewise suffer an accessory penalty consisting of disqualification to occupy public office for a term double the term of the criminal penalty imposed. Section 64. Restitution. Pursuant to the exercise of its quasi-judicial functions, the Commission shall award indemnity to an aggrieved party on the basis of the provisions of the New Civil Code. Any complaint filed by a data subject shall be subject to the payment of filing fees, unless the data subject is an indigent.

Section 65. Fines and Penalties. Violations of the Act, these Rules, other issuances and orders of the Commission, shall, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent ban on the processing of personal data, or payment of fines, in accordance with a schedule to be published by the Commission.

Rule XIV. Miscellaneous Provisions

Section 66. Appeal. Appeal from final decisions of the Commission shall be made to the proper courts in accordance with the Rules of Court, or as may be prescribed by law.

Section 67. Period for Compliance. Any natural or juridical person or other body involved in the processing of personal data shall comply with the personal data processing principles and standards of personal data privacy and security already laid out in the Act. Personal information controllers and Personal Information processors shall register with the Commission their data processing systems or automated processing operations, subject to notification, within one (1) year after the effectivity of these Rules. Any subsequent issuance of the Commission, including those that implement specific standards for data portability, encryption, or other security measures shall provide the period for its compliance. For a period of one (1) year from the effectivity of these Rules, a personal information controller or personal information processor may apply for an extension of the period within which to comply with the issuances of the Commission. The Commission may grant such request for good cause shown.

Section 68. Appropriations Clause. The Commission shall be provided with appropriations for the performance of its functions which shall be included in the General Appropriations Act. Section 69. Interpretation. Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner that would uphold the rights and interests of the individual about whom personal data is processed.

Section 70. Separability Clause. If any provision or part hereof is held invalid or unconstitutional, the remainder of these Rules or the provision not otherwise affected shall remain valid and subsisting.

Section 71. Repealing Clause. Except as otherwise expressly provided in the Act or these Rules, all other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

Section 72. Effectivity Clause. These Rules shall take effect fifteen (15) days after its publication in the Official Gazette.

Approved:
Promulgated: August 24, 2016
(Sgd.) RAYMUND E. LIBORO, Privacy Commissioner
(Sgd.) IVY D. PATDU, Deputy Privacy Commissioner
(Sgd.) DAMIAN DOMINGO O. MAPA, Deputy Privacy Commissioner

ANNEX B: DATA PRIVACY NOTICE

DATA PRIVACY NOTICE

UNIVERSITY OF SOUTHERN MINDANAO (USM) commits to protect the privacy of its data subjects, and ensures the safety and security of personal data under its control and custody. This policy provides information on what personal data is gathered by USM about its current, past, and prospective students, how it will use and process this, how it will keep this secure, and how it will dispose of it when it is no longer needed. This information is provided in compliance with the Philippine Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA) and its Implementing Rules and Regulations (DPA-IRR). It lays out USM's data protection practices designed to safeguard the personal data of individuals it deals with, and also to inform such individuals of their rights under the Act.

Privacy Notice on Information Collected

USM collects, stores, and processes personal data from its current, past and prospective students, starting with the information provided at application through to information collected throughout the whole course of their stay in the university. This will include:

1. Contact information, such as, name, addresses, telephone numbers, email addresses and other contact details
2. Personal information, such as date and place of birth, nationality, immigration status, religion, civil status, student ID, government-issued IDs, web information, recommendations and assessment forms from previous schools, etc.
3. Family background, including information on parents, guardians, siblings, etc.
4. Photographic and biometric data, such as, photos, CCTV videos, fingerprints, handwriting and signature specimens;
5. Student's school works, including data gathered using third party online learning tools, such as, Turnitin, Virtual Learning Environment, among others.
6. Health records, psychological evaluation results, disciplinary records, and physical fitness information
7. Personal Data Sheet of students, which includes interviews, entrance exam results, guidance assessments, special needs, behavioral information, etc.
8. Permanent Student Academic Records, including transcripts and the academic history of the student at USM
9. Student extra-curricular activities, resumés, job interview forms
10. Financial and billing information

Use of Information

The collected personal data is used solely for the following purposes:

1. Processing of admission application and student selection (and to confirm the identity of prospective students and their parents)
2. Verifying authenticity of student records and documents
3. Processing of scholarship applications and its on-going requirements
4. Processing of enrollment and registration
5. Supporting student learning, and validating students' program of study based on curriculum requirements, and other activities and experiences forming part of the student's formation and education
6. Supporting the student's well-being and providing medical services and guidance counselling
7. Monitoring and reporting on student progress; processing of evaluations, exam results, and grades
8. Monitoring and ensuring the safety of all students within the USM campus
9. Processing and generating statements of accounts
10. Processing of application for graduation
11. Evaluation for board examinations

12. Documentation of students' data for accreditation, professional development of teachers and staff, and research, e.g., evaluation studies by the research desk, action research by teachers, etc.
13. Posting or displaying of academic and non-academic achievements within the USM premises and/or its official website and social media accounts
14. Marketing and promoting USM, its students, employees, and other academic and non-academic student and/or school activities inside and outside the campus
15. Providing Library services, running an outreach/extension program, job postings, internships, employment

Information Sharing

Personal data under the custody of USM shall be disclosed only to authorized recipients of such data. Otherwise, we will share your personal data with third parties, other than your parents and/or guardian on record for minors, only with your consent, or when required or permitted by our policies and applicable law, such as with:

a. Regulatory authorities, courts, and government agencies, e.g., Commission on Higher Education, Department of Education, Civil Service Commission, etc.
b. The AACCUP, a service organization which accredits academic programs that meet commonly accepted standards of quality education.
c. Business partners and other academic linkages who provide internships and job opportunities to our graduates

Data Transfer

Where USM considers it necessary or appropriate, for the purposes of data storage, processing, providing any service or product on our behalf to you, or implementing an academic linkage program, we may transfer your personal data to third parties within or outside of the Philippines, under conditions of confidentiality and similar levels of security safeguards.

Security

We continue to implement organizational, administrative, technical, and physical security measures to safeguard your personal data. Only authorized personnel have access to your personal data, the exchange of which (mainly within campus) is facilitated through internal shared servers, email, and paper files. Should third parties need access to your personal data, we require some form of data sharing agreement with them, in compliance with the DPA and the DPA-IRR. Your paper and digital files are securely stored: employing physical security to safeguard the paper files and technical security to protect the digital files.

Retention of Information

We keep your paper and digital files only for as long as necessary. The following are the provisions of retention for certain data and documents containing personal data:

1. The Permanent Student Academic Records are kept by the Records Office or the Higher Education (HED) Registrar's Office for 75 years after last graduation from USM.
2. Admission files are kept for five years.
3. Application forms and documents of unsuccessful applicants are kept by the Admissions Office for five years
4. Scholarship application forms and supporting documentation are kept by the Office of Student Affairs for four years, or until the scholar graduates.
5. Student disciplinary records are stored by the Office of Student Affairs five years after graduation.
6. The class records are kept for one year after graduation.
7. Non-academic records, e.g., service records for scholars, extra-curricular activities, emergency contact forms, etc. are kept for five years.
8. Financial and billing information are kept by the Finance Offices for 10 years.

9. The Clinic retains health records for five years after graduation.
10. CCTV cameras are the responsibility of facilities in the University; some cameras have memory for a month of CCTV videos, and older ones for less. The cameras run continuously on a rolling basis, where older videos are overwritten as the memory fills up.

When your personal data is no longer needed, we take reasonable steps to securely destroy such information or permanently de-identify it. Paper files are securely shredded; and electronic information is deleted.

Your rights

You have the right to be informed, object to processing, access and rectify, suspend or withdraw your personal data, including any such information held by third parties, with whom USM have a data sharing agreement; and be indemnified in case of damages pursuant to the provisions of the DPA and the DPA-IRR.

If you want to exercise any of your rights, or if you have any questions about how we process your personal data, please contact USM's Data Protection Officer, through the following channels:

Email: dpo@usm.edu.ph
Call: (064) 572-2854
Write to:

The Data Protection Officer
Administration Building, University of Southern Mindanao
9407 Kabacan, Cotabato
dpo@usm.edu.ph

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the National Privacy Commission.

ANNEX C. **CONSENT FORM FOR STUDENTS OF THE UNIVERSITY**

STUDENT CONSENT FORM FOR THE PROCESSING, RELEASE AND RETENTION OF PERSONAL INFORMATION

I, _____, am fully aware that **University of Southern Mindanao (USM)** or its designated representative is duty bound and obligated under the Data Privacy Act of 2012 to protect all my personal and sensitive information that it collects, processes, and retains upon my enrolment and during my stay in the University.

Student personal information includes any information about my identity, academic standing, medical conditions, or any document containing my identity. This includes, but not limited to, my name, address, names of my parents or guardians, date of birth, grades, attendance, disciplinary records, and other information necessary for basic administration and instruction.

I understand that my personal information cannot be disclosed without my consent. I understand that the information that was collected and processed relates to my enrolment and to be used by USM to pursue its legitimate interests as an educational institution. Likewise, I am fully aware that USM may share such information to affiliated or partner organizations as part of its contractual obligations, or with government agencies pursuant to law or legal processes. In this regard, I hereby allow USM to collect, process, use and share my personal data in the pursuit of its legitimate interests as an educational institution.

Finally, should I commit any misconduct or should there be a complaint filed against me, before the Office of Student Affairs Office (OSA) or Student Disciplinary Board (SDB) by reason of violation of the provisions of the Student Manual or any laws or ordinances, I hereby authorize and give my full consent in favor of the University to inform my parents, guardian, representative or whoever person is in charge of providing care or custody for me.

Upon submission of this form, I hereby give my consent for the processing, release, and retention of personal information.

_____

PRINTED NAME AND SIGNATURE

_____

DATE SIGNED

ANNEX D. DATA INQUIRY/ACCESS REQUEST FORM

DATA PROTECTION INQUIRY/DATA ACCESS REQUEST FORM

Under the terms of the Data Privacy Act of 2012, data subjects are entitled to request details of any personal data that is being kept about them. The University needs to be assured of the data subject's identity before that data is released. The University holds personal records in different parts of its organization. To assist us in providing the information you require, please answer the following questions:

First Name, Middle Name, Last Name _____

Contact Number/s _____

Details of Data Request or Data Inquiry

Please specify the personal data to which you require access (identifying any specific documents) and the data location, where possible (e.g. Office, College/Department HR, etc.) Please also specify the time period covered by your request.

NAME OF DOCUMENT	TIME PERIOD COVERED

Continue on additional sheets, if necessary.

Signature: _____ Date: _____

You must provide a photocopy of a valid evidence of your identity, (University I.D./valid library card, driver's license, passport, birth certificate, etc. when making a request.

ANNEX E. NON-DISCLOSURE AGREEMENT FOR EMPLOYEES OF THE UNIVERSITY

NON-DISCLOSURE AGREEMENT FOR EMPLOYEES OF THE UNIVERSITY

KNOW ALL MEN BY THESE PRESENTS:

I, <insert full name>, <insert nationality>, of legal age and with residence at <insert address>, after being sworn in accordance with law, hereby declare that:

I am [insert title/position] of [office/unit/center] of the University of Southern Mindanao ("University").

1. *Definition of Confidential Information.* In the course of my engagement and/or in the performance of my functions, the University, its officers and authorized representatives, including affiliates and other third parties performing services for or on its behalf, may disclose to me confidential information consisting of personal data, analyses, computer files whether or not reduced to written form, compilations, memoranda, notes, reports, studies, data, drawings, films, processes, business strategies, information and documentation of all kinds including copies, extracts and summaries thereof and all other material containing or based in whole or in part on any such information, disclosed by or stored in the databases of the University in whatsoever form whether written, oral, electronic or otherwise, directly or indirectly to me or which comes into my possession or knowledge in connection with my engagement and/or work for the University, with or without "Confidential" label, before or after the date of this Agreement ("Confidential Information").

2. *Obligations*.

I undertake to maintain in confidence all Confidential Information, to take all necessary measures to prevent unauthorized access thereto, and to exercise the same level of security measures and degree of care as may be necessary to keep the confidentiality thereof.

a. I will not, without the prior written consent of the University, disclose the Confidential Information. Any breach of such obligation of confidentiality shall be deemed to be a breach of this Agreement.
b. I will not use or permit the use of the Confidential Information disclosed to me other than in connection with my engagement and/or work for the University.
c. I will not copy, reproduce, or reduce into writing any material part of the Confidential Information except as may be reasonably necessary to my engagement and/or work for the University.
d. I will not, without the prior written consent of the University, directly or indirectly initiate, solicit, negotiate, contract, or enter into any business transactions, agreements, or undertakings that will utilize the Confidential Information by exploiting or deriving any undue benefit therefrom.
e. Upon the written request of the University, I undertake to return and/or destroy all Confidential Information and certify in writing to the University that its request has been complied with.

3. *Warranties*. I acknowledge that the University makes no representation or warranty as to the accuracy or completeness of the Confidential Information, which it has provided, and that the University shall not be liable for damages arising out of or in connection with my use of Confidential Information.

4. *Licenses and Property Rights*. I acknowledge that the University reserves all rights relating to the Confidential Information and no rights or obligations other than those it has expressly provided are granted and that no license is granted to me, directly or indirectly, under any patent, invention, copyright or other intellectual or industrial property of the University.

5. *Time Periods*. I further agree that the confidentiality obligations in this the Agreement shall survive the tenure of my employment/engagement with the University, unless otherwise provided in writing by the University.

6. *Remedies*. I understand that, without prejudice to any other rights or remedies that the University may have, the University shall be entitled to seek injunction, its equivalent or similar remedy for any threatened or actual breach of this Agreement.

7. *Condition of Engagement*. I further understand that strict compliance with this Agreement is a condition of my engagement/work and any breach of this Agreement may be regarded as an infringement of my terms of engagement/work.

8. *Severability*. I acknowledge that if the court finds any provision of this Agreement invalid or unenforceable, such court decision shall not affect the remainder of this Agreement and shall be interpreted to the best interest of the University.

9. *Integration*. I understand that this Agreement expresses the complete understanding of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations, and understandings. This Agreement may not be amended except in a writing signed by both parties.
Waiver. Finally, I acknowledge that the failure to exercise any provision in this Agreement shall not constitute a waiver of prior or subsequent rights.
IN WITNESS WHEREOF, I have affixed my signature to this Agreement this (date) at (place), Philippines.

Noted by

Signature over Printed Name	Signature over Printed Name of Immediate Supervisor
Title / Designation	Title / Designation
Office / Unit	Office / Unit

Witnessed by:

Signature over Printed Name	Signature over Printed Name

Republic of the Philippines
Congress of the Philippines
Metro Manila
Fifteenth Congress
Second Regular Session

Begun and held in Metro Manila, on Monday, the twenty-fifth day of July, two thousand eleven.

[REPUBLIC ACT NO. 10173]

AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

Be it enacted, by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I
GENERAL PROVISIONS

SECTION 1. *Short Title.* – This Act shall be known as the "Data Privacy Act of 2012".

SEC. 2. *Declaration of Policy.* – It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

SEC. 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

(a) *Commission* shall refer to the National Privacy Commission created by virtue of this Act.

(b) *Consent of the data subject* refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him 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.

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

(d) *Direct marketing* refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals.

(e) *Filing system* refers to any act 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.

(f) *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 message, or electronic document.

(g) *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.

(h) *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.

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

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

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

(l) *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.

SEC. 4. *Scope.* – This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph: *Provided,* That the requirements of Section 5 are complied with.

This Act does 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;

(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;

(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 this Act 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.

SEC. 5. *Protection Afforded to Journalists and Their Sources.* – Nothing in this Act shall be construed as to have amended or repealed the provisions of Republic Act No. 53, which affords the publishers, editors or duly accredited reporters of any newspaper, magazine or periodical of general circulation protection from being compelled to reveal the source of any news report or information appearing in said publication which was related in any confidence to such publisher, editor, or reporter.

SEC. 6. *Extraterritorial Application.* – This Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:

(a) The act, practice or processing relates to personal information about a Philippine citizen or a resident;

(b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:

(1) A contract is entered in the Philippines;

(2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and

(3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and

(c) The entity has other links in the Philippines such as, but not limited to:

(1) The entity carries on business in the Philippines; and

(2) The personal information was collected or held by an entity in the Philippines.

Back To Top

CHAPTER II
THE NATIONAL PRIVACY COMMISSION

SEC. 7. *Functions of the National Privacy Commission.* – To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent body to be known as the National Privacy Commission, winch shall have the following functions:

(a) Ensure compliance of personal information controllers with the provisions of this Act;

(b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided,* That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act;

(c) Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;

(d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;

(e) Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to this Act;

(f) Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;

(g) Publish on a regular basis a guide to all laws relating to data protection;

(h) Publish a compilation of agency system of records and notices, including index and other finding aids;

(i) Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act;

(j) Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers:*Provided,* That the privacy codes shall adhere to the underlying data privacy principles embodied in this Act: *Provided, further,*That such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller. For this purpose, the Commission shall consult with relevant regulatory

agencies in the formulation and administration of privacy codes applying the standards set out in this Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law: *Provided, finally.* That the Commission may review such privacy codes and require changes thereto for purposes of complying with this Act;

(k) Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person;

(l) Comment on the implication on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions and interpret the provisions of this Act and other data privacy laws;

(m) Propose legislation, amendments or modifications to Philippine laws on privacy or data protection as may be necessary;

(n) Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection;

(o) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

(p) Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and

(q) Generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.

SEC. 8. *Confidentiality.* – The Commission shall ensure at all times the confidentiality of any personal information that comes to its knowledge and possession.

SEC. 9. *Organizational Structure of the Commission.* – The Commission shall be attached to the Department of Information and Communications Technology (DICT) and shall be headed by a Privacy Commissioner, who shall also act as Chairman of the Commission. The Privacy Commissioner shall be assisted by two (2) Deputy Privacy Commissioners, one to be responsible for Data Processing Systems and one to be responsible for Policies and Planning. The Privacy Commissioner and the two (2) Deputy Privacy Commissioners shall be appointed by the President of the Philippines for a term of three (3) years, and may be reappointed for another term of three (3) years. Vacancies in the Commission shall be filled in the same manner in which the original appointment was made.

The Privacy Commissioner must be at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, and a recognized expert in the field of information technology and data privacy. The Privacy Commissioner shall enjoy the benefits, privileges and emoluments equivalent to the rank of Secretary.

The Deputy Privacy Commissioners must be recognized experts in the field of information and communications technology and data privacy. They shall enjoy the benefits, privileges and emoluments equivalent to the rank of Undersecretary.

The Privacy Commissioner, the Deputy Commissioners, or any person acting on their behalf or under their direction, shall not be civilly liable for acts done in good faith in the performance of their duties. However, he or she shall be liable for willful or negligent acts done by him or her which are contrary to law, morals, public policy and good customs even if he or she acted under orders or instructions of superiors: *Provided,* That in case a lawsuit is filed against such official on the subject of the performance of his or her duties, where such performance is lawful, he or she shall be reimbursed by the Commission for reasonable costs of litigation.

SEC. 10. *The Secretariat.* – The Commission is hereby authorized to establish a Secretariat. Majority of the members of the Secretariat must have served for at least five (5) years in any agency of the government that is involved in the processing of personal information including, but not limited to, the following offices: Social Security System (SSS), Government Service Insurance System (GSIS), Land Transportation Office (LTO), Bureau of Internal Revenue (BIR), Philippine Health Insurance Corporation (PhilHealth), Commission on Elections (COMELEC), Department of Foreign Affairs (DFA), Department of Justice (DOJ), and Philippine Postal Corporation (Philpost).

Back To Top

CHAPTER III
PROCESSING OF PERSONAL INFORMATION

SEC. 11. *General Data Privacy Principles.* – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

Personal information must, be:,

(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 lie 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.

The personal information controller must ensure implementation of personal information processing principles set out herein.

SEC. 12. *Criteria for Lawful Processing of Personal Information.* – 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 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.

SEC. 13. *Sensitive Personal Information and Privileged Information.* – 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;

(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.

SEC. 14. *Subcontract of Personal Information. – A* personal information controller may subcontract the processing of personal information: *Provided,* That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws.

SEC. 15. *Extension of Privileged Communication.* – Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered on privileged information is inadmissible.

Back To Top

CHAPTER IV
RIGHTS OF THE DATA SUBJECT

SEC. 16. *Rights of the Data Subject.* – The data subject is entitled 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 Commission.

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of 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 legal obligation;

(c) Reasonable access to, upon demand, the following:

(1) Contents of his or her personal information that were processed;

(2) Sources from which personal information were obtained;

(3) Names and addresses of recipients of the personal information;

(4) Manner by which such data were processed;

(5) Reasons for the disclosure of the personal information to recipients;

(6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

(7) Date when his or her personal information concerning the data subject were last accessed and modified; and

(8) The designation, or name or identity and address of the personal information controller;

(d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: *Provided,* That the third parties who have previously received such processed personal information shall he informed of its inaccuracy and its rectification upon reasonable request of the data subject;

(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

SEC. 17. *Transmissibility of Rights of the Data Subject.* – The lawful heirs and assigns of the data subject may invoke the rights of the data subject for, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

SEC. 18. *Right to Data Portability.* – The data subject shall have 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 Commission may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer.

SEC. 19. *Non-Applicability.* – The immediately preceding sections are not applicable if the processed personal information are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: *Provided,* That the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections 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.

Back To Top

CHAPTER V
SECURITY OF PERSONAL INFORMATION

SEC. 20. *Security of Personal Information.* – (a) The personal information controller must 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.

(b) The personal information controller 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.

(c) 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 as the 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.

(d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

(e) The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

(f) The personal information controller shall promptly notify the Commission and affected data subjects when 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 the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive

personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only 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.

(1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information.

(2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.

(3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Back To Top

CHAPTER VI
ACCOUNTABILITY FOR TRANSFER OF PERSONAL INFORMATION

SEC. 21. *Principle of Accountability.* – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.

(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

Back To Top

CHAPTER VII
SECURITY OF SENSITIVE PERSONAL
INFORMATION IN GOVERNMENT

SEC. 22. *Responsibility of Heads of Agencies.* – All sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements

mentioned herein while the Commission shall monitor the compliance and may recommend the necessary action in order to satisfy the minimum standards.

SEC. 23. *Requirements Relating to Access by Agency Personnel to Sensitive Personal Information.* – (a) On-site and Online Access – Except as may be allowed through guidelines to be issued by the Commission, no employee of the government shall have access to sensitive personal information on government property or through online facilities unless the employee has received a security clearance from the head of the source agency.

(b) Off-site Access – Unless otherwise provided in guidelines to be issued by the Commission, 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 agency in accordance with the following guidelines:

(1) Deadline for Approval or Disapproval – In the case of any request submitted to the head of an agency, such head of the 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;

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

(3) 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 Commission.

The requirements of this subsection shall be implemented not later than six (6) months after the date of the enactment of this Act.

SEC. 24. *Applicability to Government Contractors.* – In entering into any contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, an agency shall require a contractor and its employees to register their personal information processing system with the Commission in accordance with this Act and to comply with the other provisions of this Act including the immediately preceding section, in the same manner as agencies and government employees comply with such requirements.

Back To Top

CHAPTER VIII
PENALTIES

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 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) 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 personal sensitive 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 (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) 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 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

(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 (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

SEC. 27. *Improper Disposal of Personal Information and Sensitive Personal Information.* – (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 (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) 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 (Php100,000.00) but not more than One million pesos (Php1,000,000.00) 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.

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 (Php500,000.00) but not more than One million pesos (Php1,000,000.00) 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 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) 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 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) 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.

SEC. 30. *Concealment of Security Breaches Involving Sensitive Personal Information.* – 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 (Php500,000.00) but not more than One million pesos (Php1,000,000.00) 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.

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) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

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 he subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

(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 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

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 (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

SEC. 34. *Extent of Liability.* – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

SEC. 35. *Large-Scale.* – The maximum penalty in the scale of penalties respectively provided for the preceding offenses shall be imposed when the personal information of at least one hundred (100) persons is harmed, affected or involved as the result of the above mentioned actions.

SEC. 36. *Offense Committed by Public Officer.* – When the offender or the person responsible for the offense is a public officer as defined in the Administrative Code of the Philippines in the exercise of his or her duties, an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall he applied.

SEC. 37. *Restitution.* – Restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.

Back To Top

CHAPTER IX
MISCELLANEOUS PROVISIONS

SEC. 38. *Interpretation.* – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

SEC. 39. *Implementing Rules and Regulations (IRR).* – Within ninety (90) days from the effectivity of this Act, the Commission shall promulgate the rules and regulations to effectively implement the provisions of this Act.

SEC. 40. *Reports and Information.* – The Commission shall annually report to the President and Congress on its activities in carrying out the provisions of this Act. The Commission shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public of data privacy, data protection and fair information rights and responsibilities.

SEC. 41. *Appropriations Clause.* – The Commission shall be provided with an initial appropriation of Twenty million pesos (Php20,000,000.00) to be drawn from the national government. Appropriations for the succeeding years shall be included in the General Appropriations Act. It shall likewise receive Ten million pesos (Php10,000,000.00) per year for five (5) years upon implementation of this Act drawn from the national government.

SEC. 42. *Transitory Provision.* – Existing industries, businesses and offices affected by the implementation of this Act shall be given one (1) year transitory period from the effectivity of the IRR or such other period as may be determined by the Commission, to comply with the requirements of this Act.

In case that the DICT has not yet been created by the time the law takes full force and effect, the National Privacy Commission shall be attached to the Office of the President.

SEC. 43. *Separability Clause.* – If any provision or part hereof is held invalid or unconstitutional, the remainder of the law or the provision not otherwise affected shall remain valid and subsisting.

SEC. 44. *Repealing Clause.* – The provision of Section 7 of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", is hereby amended. Except as otherwise expressly provided in this Act, all other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

SEC. 45. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its publication in at least two (2) national newspapers of general circulation.

Back To Top

Approved,

(Sgd.) **FELICIANO BELMONTE JR.** *Speaker of the House of Representatives*

(Sgd.) **JUAN PONCE ENRILE** *President of the Senate*

This Act which is a consolidation of Senate Bill No. 2965 and House Bill No. 4115 was finally passed by the Senate and the House of Representatives on June 6, 2012.

(Sgd.) **MARILYN B. BARUA-YAP** *Secretary General House of Representatives*

(Sgd.) **EMMA LIRIO-REYES** *Secretary of the Senate*

Approved: **AUG 15 2012**

(Sgd.) **BENIGNO S. AQUINO III** *President of the Philippines*

Republic of the Philippines
UNIVERSITY OF SOUTHERN MINDANAO
Kabacan, Cotabato
Tel. No.064-572-2016
email address:vpaf@usm.edu.ph

Management System ISO 9001:2015
TÜVRheinland CERTIFIED
www.tuv.com ID 9108634167

VICE PRESIDENT FOR ADMINISTRATION AND FINANCE

MEMORANDUM No. 10
Series of 2024

TO : ALL UNIT HEADS & DCOs IN THE USM ADMINISTRATION BUILDING

SUBJECT : TRAINING ON THE CATEGORIZATION OF OFFICE DOCUMENTS AND RECORDS

DATE : FEBRUARY 19, 2024

The team responsible for University Records Management and Archiving, under the guidance of the University President, is scheduled to carry out " Digital Archiving Training Workshop" tomorrow at 1:00 p.m., February 20, 2024, in the Admin Sky Room. Records Office Personnel, Heads of offices and DCOs are encouraged to participate in this crucial training, aimed at improving personnel skills in digital archiving. This training is vital for the ongoing restructuring of the university's records and management system.

Your presence is highly appreciated.

EIMER M. ESTILLOSO, EdD
Vice-President for Administration and Finance Office