AFP FREEDOM OF INFORMATION MANUAL

Executive Order No. 2
Series of 2016

AFP FOI MANUAL
(AS OF JUNE 5, 2017)

Armed Forces of the Philippines Freedom of Information Manual

Disclaimer: This version of the AFP FOI Manual is subject to amendment.

TABLE OF CONTENTS

Section	*Topic*	*Page*
	CHAPTER 1 – INTRODUCTION	
1.	General	5
2.	Rationale	5
3.	Structure of the Manual	6
4.	Coverage of the Manual	6
	CHAPTER 2 – GENERAL PROVISIONS	
1.	Legal Bases	6
2.	Guiding Principles	7
3.	Definition of Terms	9
4.	Promotion of Openness in Government	14
5.	Protection of Privacy	15
6.	Limitations	15
	CHAPTER 3 – AFP FOI AUTHORITIES	
1.	FOI Receiving Officer	16
2.	FOI Cognizant Office/Unit	17
3.	FOI Decision Maker	17
4.	Central Appeals and Review Committee	18
	CHAPTER 4 – CLASSIFICATION OF MILITARY DOCUMENTS	18
	CHAPTER 5 – AFP FOI PROCEDURE	
1.	Receipt of Request for Information	20
2.	Initial Evaluation of the FOI Request	22
3.	Transmittal of the FOI Request to the COU	22
4.	Approval or Denial of the Issuance of FOI Request	23
5.	Transmittal of the FOI Request to the Requestor	23

6. Notice for an Extension of Time 24

CHAPTER 6 – REMEDIES IN CASE OF DENIAL 24

CHAPTER 7 – FOI REQUEST MONITORING 25

CHAPTER 8 – AFP FOI DOCUMENT INVENTORY 26

CHAPTER 9 – FEES 26

CHAPTER 10 – UNDERTAKING 26

CHAPTER 11 – ADMINISTRATIVE LIABILITY 27

CHAPTER 12 – AFP FOI TRAININGS 27

CHAPTER 13 – PERIODIC REVIEW 28

CHAPTER 14 – FINAL PROVISIONS 28

ANNEXES

a. Executive Order No. 02, series of 2016 dated July 23, 2016 titled "Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies of Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor"

b. Memorandum from the Executive Secretary, Office of the President of the Philippines, dated November 24, 2016 with the subject "Inventory of Exceptions to Executive Order No. 2, series of 2016"

c. Memorandum Circular No. 78, series of 1964 dated August 14, 1964 titled "Promulgating Rules Governing Security of Classified Matter in Government Offices", as amended by Memorandum Circular No. 196, series of 1968 dated July 19, 1968

d. Republic Act No. 10173 dated July 25, 2011 known as the "Data Privacy Act of 2012"

e. Detailed FOI Request Process

f. FOI Request Form

g. FOI Appeal Template

h. FOI Request Flow Chart

CHAPTER 1
INTRODUCTION

Section 1-1 General

1. Section 3, Article II of the 1987 Philippine Constitution states that "the Armed Forces of the Philippines is protector of the people and the State. Its goal is to secure the sovereignty of the State and the integrity of the national territory." In extraordinary situations, the Armed Forces of the Philippines (AFP) may also be called upon to protect the people when ordinary law and enforcement forces need assistance.

2. In line with Executive Order No. 02, series of 2016 dated July 23, 2016 titled "Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies of Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor," the AFP formulated the AFP Freedom of Information (FOI) Manual which shall define the balance between the people's right to information and the AFP's obligation to provide accurate, reliable and timely information without compromising national, operational, and personnel security.

3. As such, classified military information is treated as national security assets that need to be conferred with varying degrees of protection in order to prevent enemies of the Filipino people from gaining undue advantage that can undermine the sovereignty of the Philippines and the integrity of the national territory.

Section 1-2 Rationale

1. This Manual aims to assist the public and guide the Armed Forces of the Philippines (AFP) in the implementation of E. O. No. 2, s. of 2016 on FOI.

Section 1-3 Structure of the Manual

1. The AFP FOI Manual sets out the definition of terms, standard operating procedures, rules, remedies, fees, and administrative liability relative to the AFP's implementation of FOI. This AFP FOI Manual also provides the relevant forms and annexes.

Section 1-4 Coverage

1. The AFP FOI Manual covers all requests for information made through the FOI mechanism directed to the AFP.

CHAPTER 2
GENERAL PROVISIONS

Section 2-1 Legal Bases

1. This Manual is based on the following laws, rules, and regulations:

a. The 1987 Philippine Constitution

1) Section 7, Article III: "The right of the people to information on matters of public concern shall be recognized. Access to official 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, shall be afforded the citizen, subject to such limitations as may be provided by law."

2) Section 28, Article II: "The State adopts the policy of full public disclosure of all its transactions involving public interest."

b. Executive Order No. 02, series of 2016 dated July 23, 2016 titled "Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies of Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor." ***(Annex A)***

c. Memorandum from the Executive Secretary, Office of the President of the Philippines, dated November 24, 2016 with the subject "Inventory of Exceptions to Executive Order No. 2, series of 2016." ***(Annex B)***

d. Memorandum Circular No. 78, series of 1964 dated August 14, 1964 titled "Promulgating Rules Governing Security of Classified Matter in Government Offices", as amended by Memorandum Circular No. 196, series of 1968 dated July 19, 1968. ***(Annex C)***

e. Republic Act No. 10173 dated July 25, 2011 known as the "Data Privacy Act of 2012." ***(Annex D)***

Section 2-2 Guiding Principles

1. This Manual adheres to the following principles:

a. **Maximum Disclosure**. All information or documents issued by or under the custody of AFP which are of public interest shall be disclosed to the public, provided said disclosure does not affect national, operational, and personnel security matters.

b. **List of Exceptions**. The exceptions to access to information or documents held by the AFP which are of public interest shall be stated clearly and be free of any ambiguity.

c. **Classification Categories**. All information or documents requiring protection in the interest of national, operational, and personnel security shall be classified and limited only to four (4) categories: **Top Secret**, **Secret**, **Confidential**, and **Restricted**.

d. **Clear Procedure to Facilitate Access**. All requests for information or documents directed to the AFP shall go through the procedure discussed in Chapter 5.

e. **Access Requirements**. Release of requested information or documents shall be allowed after criteria set forth in this Manual are met. In addition, the AFP FOI Cognizant Office/Unit (COU) reserves the right to require the security clearance of the requesting party prior to the release of information or document requested.

f. **Sanitization**. Requests for information or document shall only be limited to the information necessary to meet the purpose stated in the completed requesting party's FOI Request Form. As such, said information or document requested may be sanitized prior to its release.

g. **Availability of an Appeal**. A privilege afforded to the requestor for review of the decision made by the agency through its Central Appeals and Review Committee (CARC).

h. **Sensitive Personal Information**. As defined in the Data Privacy Act of 2012 (Republic Act No. 10173) shall refer 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 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.

Section 2-3 Definition of Terms

1. For purposes of this Manual, the following terms are hereby defined as follows:

a. **Administrative FOI Appeal**. An independent review of the initial determination made in response to an FOI request. Requesting parties who are dissatisfied with the response to their initial request have a right to appeal that initial determination to an office within the agency, which will then conduct an independent review.

b. **Annual FOI Report**. A report to be filed each year with the Presidential Communications Operations Office (PCOO) by all government agencies detailing the administration of the FOI. Annual FOI Reports contain detailed statistics on the number of FOI requests and appeals received, processed, and pending at each government office.

c. **Classified Matters**. Information and materials categorized by the responsible classifying authority based on its importance. Classified military information (CMI), includes but is not limited to, all information and materials that are within the scope of national, operational, and personnel security.

d. **Compromise**. For this Manual, it shall be understood as a loss of security which would result to the exposure of CMI to an unauthorized person.

e. **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.”

d. **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.

e. **eFOI.gov.ph**. The website that serves as the government's comprehensive FOI website for all information on the FOI. Among many other features, eFOI.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. eFOI.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.

f. **Exceptions**. Information that cannot be released and disclosed in response to an FOI request because they are protected by the Constitution, laws or jurisprudence.

g. **FOI Contact**. The name, address, and phone number of specific personnel at each government office where you can make an FOI request.

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

h. **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.

j. **Frequently Requested Information**. Information released in response to an FOI request that the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records.

k. **Freedom of Information FOI (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, series of 2016. 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.

l. **Full Denial**. When the AFP cannot release any records in response to an FOI request since the requested information is exempt from disclosure in its entirety or no records responsive to the request could be located.

m. **Full Grant**. When a government office is able to disclose all records in full in response to an FOI request.

n. **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.

o. **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.

p. **Multi-Tracking 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.

q. **National Security**. The state or condition wherein the nation's sovereignty and territorial integrity, the people's well-being, core values, and way of life, and the State and its institutions, are protected and enhanced.

r. **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.

s. **Open Data**. Refers to publicly available data structured in a way that enables the data to be fully discoverable and usable by end users.

t. **Order of Battle**. Pertains to the hierarchical organization, command structure, strength, disposition of forces, units, formations, and equipment of a military force.

u. **Partial Grant/Partial Denial of Information**. When a government office is able to disclose only portions of the records in response to an FOI request.

v. **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.

w. **Perfected Request**. An FOI request, which reasonably describes the records sought and is made in accordance with the government office's regulations.

x. **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.

y. **Processed Request or Processed Appeal**. Requests or appeals where the agency has completed its work and sent a final response to the requester.

z. **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.

aa. **Public Service Contractor**. Shall be defined as a private entity that has dealings, contracts, or transactions of whatever form or kind with the government or a government agency or office that utilizes public funds.

bb. **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.

cc. **Received Request or Received Appeal**. An FOI request or administrative appeal that an agency has received within a fiscal year.

dd. **Referral**. When a government office locates a record that originated from, or is of 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.”

ee. **Security Clearance**. An administrative determination of eligibility for a particular individual from a security standpoint to access classified matter of a specific category.

ff. **Simple Request**. An FOI request that an agency anticipates will involve either a small volume of material or material which can be processed relatively quickly.

Section 2-4 Promotion of Openness in Government

1. Duty to Publish Information. The AFP shall regularly publish, print, and disseminate at no cost to the public and in an accessible form, in conjunction with Republic Act 9485 (Anti-Red Tape Act of 2007), and through their website, timely, true, accurate, and updated key information including, but not limited to:

a. A description of its mandate, structure, powers, functions, duties, and decision-making processes;

b. A description of the frontline services it delivers and the procedure and length of time by which they may be availed of;

c. The names of its key officials, their powers, functions and responsibilities, and their profiles;

d. Work programs, development plans, investment plans, projects, performance targets and accomplishments, and budgets, revenue allotments and expenditures;

e. Important rules and regulations, orders or decisions;

f. Current and important databases and statistics that it generates;

g. Bidding processes and requirements; and

h. Mechanisms or procedures by which the public may participate in or otherwise influence the formulation of policy or the exercise of its powers.

2. Accessibility of Language and Form. The AFP shall endeavor to translate key information into the major Filipino languages and present them in popular form and means.

3. Keeping of Records. The AFP shall create and/or maintain in appropriate formats, accurate, and reasonably complete documentation or records, policies, transactions, decisions, resolutions, enactments, actions, procedures, operations, activities, communications and documents received or filed and the data generated or collected.

4. Security of Classification. Memorandum Circular No. 78, series of 1964 dated August 14, 1964 titled “Promulgating Rules Governing Security of Classified

Matter in Government Offices", as amended by Memorandum Circular No. 196, series of 1968 dated July 19, 1968 shall remain effective with respect to requested information covered by the said circular. ***(Annex C)***

SECTION 2-5 Protection of Privacy

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

a. The AFP shall ensure that personal information, *including sensitive personal information*, in its custody or under its control is disclosed only as permitted by existing laws;

b. The AFP shall protect personal information, *including sensitive personal information*, in its custody or under its control by making reasonable security arrangements against unauthorized access, leaks, or premature disclosure; and

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

Section 2-6 Limitations

1. The right of access to information is without prejudice to the right of the AFP to deny such access due to the existence of the following:

a. The identity of the requesting party is fictitious or illegitimate based on the credentials provided by him/her;

b. Said request is prompted only by sheer idle curiosity;

c. Said request is being made with a plainly discernible ulterior motive such as harassment;

d. The purpose of the said request is contrary to law, morals, good customs or public policy, or the request is for a commercial purpose; and

e. Said request will compromise national, operational, and personnel security.

2. In all instances, basic security principles, common sense, and logical interpretation of existing laws, jurisprudence, rules, and regulations shall be applied.

CHAPTER 3
AFP FOI AUTHORITIES

Section 3-1 FOI Receiving Officer

1. FOI Receiving Officer (FRO). The AFP FRO shall be the Chief, Public Affairs Office, AFP (C, PAO AFP). The FRO can be contacted through the following:

a. Address: Public Affairs Office
GHQ Grandstand, De Jesus Avenue
Camp General Emilio Aguinaldo, Quezon City

b. Contact numbers: 911-6001 local 6700
09177776034 / 09399908691

c. E-mail address: paoafp@gmail.com

2. Any changes to the foregoing contact information of the FRO shall be posted on the official AFP website at http://www.afp.mil.ph.

3. The functions of the FRO are the following:

a. Receive, on behalf of the AFP, all requests for information;

b. Assess if the requesting party has clearly communicated its request, if the AFP can provide the information requested, or if the request is a repeat of a previous request from the same party;

c. Evaluate FOI Requests against disclosure criteria and requirements (Chapter 5, Section 2);

d. Facilitate processing of all FOI Requests;

e. Coordinate with the requesting party regarding all concerns related to the FOI Request;

f. Monitor all FOI transactions, compile relevant statistical information, and prepare all relevant reports regarding the AFP's implementation of FOI;

g. Assist the FOI Decision Maker in evaluating all FOI requests; and

h. Assist and inform the public with regard to the AFP's implementation of FOI.

4. Should an FOI Request be made through one of AFP line units, receiving units shall forward said request to PAO, AFP within one (1) day.

Section 3-2 FOI Cognizant Office/Unit

1. FOI Cognizant Office/Unit (COU). The AFP COU shall be determined by the FRO based on the nature of the information requested. The COU shall provide assistance, recommendations, and advice to the FOI Decision Maker in all matters arising from the evaluated FOI Requests based on the criteria set forth in this document.

2. As such, all AFP offices and units determined as COU shall designate their Chief, Administrative Officer as the FOI Action Officer (FAO). The FAO shall facilitate the processing of FOI Requests forwarded by the FRO. The full contact details of the COU's FAO shall be submitted regularly to the FRO. In case of changes, the COU shall immediately provide updated contact details to the FRO.

Section 3-3 FOI Decision Maker

1. The FOI Decision Maker (FDM) shall be the Chief of Staff, AFP (CSAFP). In case of CSAFP's absence or otherwise inability to act as FDM, the Vice Chief of Staff, AFP (VCSAFP) shall substitute on matters up to his level only. The FDM has the sole authority to approve or deny the release of the information requested based on the recommendations of the COU.

Section 3-4 Central Appeals and Review Committee

1. There shall be a Central Appeals and Review Committee (CARC) composed of the following:

Chairperson:

The Deputy Chief of Staff, AFP

Members:

Assistant Deputy Chief of Staff for Intelligence, AJ2
Assistant Deputy Chief of Staff for Civil-Military Operations, AJ7
Deputy Chief or Deputy Commander of the COU
Judge Advocate General

2. There shall be an FOI Appeals and Review Subcommittee (FARS) that will serve as secretariat to the CARC. It shall be composed of the Executive Officers from the Office of the Deputy Chief of Staff for Intelligence, the Office of the Deputy Chief of Staff for Civil-Military Operations, the COU, and the Office of the Judge Advocate General. The FARS shall be headed by the Executive Officer of OJ7.

3. The FARS shall review all appeals made on denied FOI Requests and evaluate the information requested and the FDM's decision. It shall then submit its recommendation to the CARC for final deliberation and approval. The CARC shall then submit its recommendation to CSAFP who shall either uphold or overturn the denial of the FOI Request. In case the CSAFP upholds the denial of the said request, the requesting party may file an appeal with the Office of the President, and may further pursue appropriate judicial action in accordance with the Rules of Court.

CHAPTER 4
CLASSIFICATION OF MILITARY DOCUMENTS

1. All information, documents, and material, in any form or of any nature, by and for the AFP or under its jurisdiction or control, and which requires protection

necessary in the interest of national security, are classified as Top Secret, Secret, Confidential, Restricted, and Open and Available Document, as the case may be.

a. **Top Secret**. These are information, documents, or material within the purview of the AFP that requires the highest degree of protection. Unauthorized disclosure of such information will cause exceptionally grave political, economic, diplomatic or military damage to the nation. This category is reserved for the State's closest secrets and shall be used with great reserve. The following are, among others, considered TOP SECRET:

1) Information, documents, or materials that may lead to a definite break in diplomatic relations, armed attack against the Philippines or her allies, war, or other situations which may adversely affect the defense of the Philippines; and

2) Information, documents, or materials that may compromise military or defense plans, intelligence operations, political or economic projects, or scientific or technological developments vital to national defense.

b. **Secret**. These are information, documents, or material within the purview of the AFP whose unauthorized disclosure would endanger national security and could cause serious injury to the interest or prestige of the nation or any governmental authority, political policies, or plans of the government. Disclosure of such information will seriously prejudice government operations or would be of great advantage to a foreign nation. The following are, among others, considered SECRET:

1) Information, documents, or materials that may jeopardize the international relations of the Philippines;

2) Information, documents, or materials that may endanger the effectiveness of a program or governmental scheme or policy of vital importance to national defense;

3) Information, documents, or materials that may compromise defense plans or scientific or technological developments important to national defense; and

4) Information, documents, or materials that may reveal important intelligence operations.

c. **Confidential**. These are information, documents, or materials within the purview of the AFP whose unauthorized disclosure would be prejudicial to the interest or prestige of the nation or any government activity, or would cause administrative embarrassment or unwarranted injury to an individual, or would be of advantage to a foreign nation.

d. **Restricted**. These are information, documents, or materials which require special protection other than that determined to be Top Secret, Secret or Confidential and whose publication or correspondence shall only be granted for official purposes only.

e. **Open and Available Data**. These are information, documents, or materials posted and publicly available in the AFP website, data.gov.ph, foi.gov.ph, or any other publicly available repository of information.

CHAPTER 5
AFP FOI PROCEDURE *(Annex E)*

Section 5-1 Receipt of Request for Information

1. The FOI Receiving Officer (FRO) shall receive the request for information from the requesting party and check its compliance with the following requirements:

a. The request must be in writing and be accomplished using the prescribed FOI Request Form. ***(Annex F)*** The request form shall be made available at the Public Affairs Office, AFP and on the AFP website;

b. Requesting party must make the request in person;

c. The request shall contain the full name and contact information of the requesting party, as well as at least two (2) government-issued identification cards (IDs) with photograph and signature;

d. The request shall reasonably describe the information requested and purpose of the request for information; and

e. The requesting party must also provide clearances from the National Bureau of Investigation (NBI), Philippine National Police (PNP), and from the Barangay where he/she resides.

2. Requests through electronic mail (e-mail) will be accommodated, provided that the requesting party submits scanned copies of the accomplished and signed FOI Request, two (2) government-issued IDs, and clearances from NBI, PNP, and his/her barangay. Further, the requesting party will still be required to appear before the FRO in person to facilitate the security clearance and answer any clarifications regarding the purpose and/or content of the request.

3. In case the requesting party is unable to make a written request because of illiteracy or disability, he or she may make an oral request which the FRO shall put in writing.

4. 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, and signature of the public officer who received it. A copy shall be given to the requesting party. The FRO shall input the details of the request into the Request Tracking System and allocate a reference number.

5. The AFP shall respond to requests within fifteen (15) working days following the date of receipt of the request. A working day is any day other than a Saturday, Sunday or a day that is declared a national public holiday in the Philippines. In computing for the period, Article 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 was physically delivered to the FRO;

b. The day on which requesting parties who have forwarded their request through e-mail have personally appeared to the FRO; or

c. If the AFP has asked the requesting party for further details to identify and locate the requested information, the date after which the necessary clarification was received.

6. Should the requested information require further clarifications to identify or locate, then the 15 working days will commence on the day after the FRO has received the required clarification from the requesting party.

7. The FRO shall make it clear to the requesting party that all information or documents released by the AFP through FOI shall not be shared or furnished to a third party without the appropriate request initiated by the former or clearance from the AFP. In case the same information will be used for another purpose, a new request shall be initiated informing the AFP of the new purpose.

Section 5-2 Initial Evaluation of the FOI Request

1. After receipt of the request for information, the FRO shall conduct an initial evaluation of the request and advise the requesting party whether or not the request shall be facilitated further by the AFP. Upon evaluation, the FRO can deny FOI requests based on any of the following grounds:

a. The FOI Request form is incomplete;

b. The information, documents, or material requested is already disclosed in the Official AFP Website, at data.gov.ph, or at any other publicly accessible repository of data;

c. The information, documents, or material requested is not in the custody of the AFP;

d. The information, documents, or material requested is substantially similar or identical to a previous request that has already been granted or denied by the AFP to the same requesting party;

e. The requesting party intends to use the requested information or document in criminal, administrative, or civil proceedings; and

f. The information, documents or material requested falls under any of the exceptions enshrined in the Constitution, existing law or jurisprudence, or is enumerated in the Inventory of Exceptions to E. O. No. 2, series of 2016 ***(Annex B)***.

Section 5-3 Transmittal of the FOI Request to the COU

1. The FRO shall transmit the endorsed request to the COU after it has passed initial evaluation. The FRO shall record the date, time, and name of the unit or office which received the request in a record book with the corresponding signature of acknowledgement of receipt of the request.

2. The COU shall take all necessary steps to locate and retrieve the requested information for release to the requesting party.

3. The COU shall communicate denial of the request to the FRO in the event that the requested information is not in its custody or if it falls under any of the exceptions enshrined in the Constitution, existing law or jurisprudence, or is CMI, as the case may be.

4. If the COU determines that a record contains information of interest to another office, the FRO shall consult with the agency concerned whether said information may be disclosed before making any final determination.

5. Should there be a need for clarification of the request or clearance of the requesting party, the FRO shall communicate notice of said extension to the requesting party. The 15-day working period for the processing of the request shall then be paused and shall recommence on the day that the required clarification is received from the requesting party.

6. The COU shall forward the requested information and recommendation for the release of information to the FDM within 10 working days from receipt of the endorsed request from the FRO.

Section 5-4 Approval or Denial of the Issuance of FOI Request

1. The CSAFP, as the Final Decision Maker (FDM), shall refer to the guidelines set forth in this Manual and the recommendations of the COU to determine whether or not to grant the FOI request. The FDM shall then inform the FRO of the action to be taken on said request.

Section 5-5 Transmittal of the FOI Request to the Requestor

1. Upon receipt of the requested information from the FDM, the FRO shall ensure that the information is complete. The FRO shall attach a cover/transmittal letter signed by the CSAFP or, in case of the CSAFP's absence, the VCSAFP, and ensure that the same be transmitted to the requesting party within 15 working days upon receipt of the request for information.

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

3. In case of denial of the request, whether 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.

Section 5-6 Notice for an Extension of Time

1. If the information requested requires extensive search of office records and facilities, examination of voluminous records, the occurrence of fortuitous events, or other analogous cases, or the COU requires security clearance for the requesting party, the concerned AFP unit or office should inform the FRO.

2. 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 in addition to the mandated fifteen (15) working days to act on the request, unless exceptional circumstances warrant a longer period.

CHAPTER 6
REMEDIES IN CASE OF DENIAL

1. Administrative FOI Appeal to the AFP Central Appeals and Review Committee (CARC):

a. A person whose request for information has been denied may file a written appeal with the AFP CARC within fifteen (15) days from notice of said denial. ***(Annex G)*** Failure to appeal after the 15-day period shall be deemed a waiver of the right to appeal.

b. The AFP CARC shall decide on the said appeal 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.

c. The denial of the FOI Request by the AFP CARC or the lapse of the period to respond to the request may be appealed further to the Office of the President under Administrative Order No. 22, series of 2011.

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

CHAPTER 7
FOI REQUEST MONITORING

1. In compliance with the provisions set forth in this Manual, the following shall be implemented:

a. The FRO shall establish a system to trace the status of all requests for information received, which may be paper-based, online, or both.

b. The FRO shall submit quarterly and annual FOI reports to the Office of the President through its Presidential Communications Operations Office (PCOO; copy furnished: Office of the Deputy Chief of Staff for Civil-Military Operations, J7). These reports shall contain the number of requests for information, documents, or materials granted or denied, and days and hours spent in the processing of FOI Requests.

CHAPTER 8
AFP FOI DOCUMENT INVENTORY

1. Every first quarter of the following year, the FRO, in coordination with the COUs, shall prepare an inventory of all information, documents, and materials in the custody of the COUs during the preceding year.

CHAPTER 9
FEES

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

2. Reasonable Cost of Reproduction and Copying of the Information: The FRO shall immediately notify the requesting party in case there shall be a reproduction and copying fee in order to provide the information. An amount of TWO PESOS (**PhP2.00**) shall be the maximum copying fee per page. The schedule of fees shall be posted by the AFP at the FRO.

3. Exemption from Fees: The AFP may exempt any requesting party from payment of fees should there be a valid reason provided justifying non-payment of the fees.

CHAPTER 10
UNDERTAKING

1. The requesting party, upon receipt of the requested information or document, acknowledges the following:

a. The information or document requested shall not be used for any purpose other than what is indicated in the request form;

b. The information or document shall not be used for any purpose that is contrary to law, public policy, public order, morals, or good customs; and

c. The information or document shall not be reproduced for any commercial use.

CHAPTER 11
ADMINISTRATIVE LIABILITY

1. Non-compliance with FOI. Failure of the AFP military personnel to comply with the provisions of this Manual shall be governed by the Articles of War while failure of the same by the AFP civilian employee shall be a ground for the following administrative penalties:

a. 1st Offense - Reprimand;
b. 2nd Offense – Suspension of one (1) day to thirty days;
c. 3rd Offense – Suspension of one (1) month to six (6) months; and
d. 4th Offense - Dismissal from the service.

2. Procedure. The Articles of War and other existing AFP Rules and Regulations shall be applicable for the military personnel while the Revised Rules on Administrative Cases in the Civil Service shall be applicable for the civilian personnel of the AFP in the disposition of administrative liability 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 anybody or agency, which provides for more stringent penalties.

CHAPTER 12
AFP FOI TRAININGS

1. The FRO, in coordination with OJ7, shall conduct executive briefings with the COUs, FDM, and CARC to apprise the key AFP FOI Authorities on their responsibilities under this Manual and to ensure that the process is correctly followed. Regular trainings for all AFP personnel shall also be conducted to raise awareness on their rights under the FOI, increase understanding of the principles and application of FOI, and familiarize them with the AFP FOI procedures.

CHAPTER 13
PERIODIC REVIEW

1. This Manual shall be subject for review in July 2019 and every three (3) years thereafter or when necessary.

CHAPTER 14
FINAL PROVISIONS

1. Funding of activities under this Manual shall be charged to the AFP's regular budget.

2. This Manual may be amended, revised or modified as necessary.

3. This Manual shall be posted on the AFP official website and shall take effect upon filing with and publication of the Office of the National Administrative Register (ONAR).

APPROVAL

This AFP Freedom of Information Manual was signed and approved on _____ by:

GEN CARLITO G GALVEZ JR AFP
Chief of Staff
Armed Forces of the Philippines

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 OF FULL PUBLIC DISCLOSURE AND TRANSPARENCY IN THE PUBLIC SERVICE AND PROVIDING GUIDELINES THEREFOR

WHEREAS, pursuant to Section 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 departments, 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 recordings, magnetic or other tapes, electronic data, computer-stored data, or 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, departments, bureaus, and instrumentalities, including government-owned or -controlled corporations, and state universities and colleges. Local government units (LGUs) are enjoined 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 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 laws or jurisprudence.

The Department 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 Department 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 as provided in Section 4 hereof.

The determination of the applicability of any of the exceptions to the request shall be the responsibility of the Head of the Office which has custody or control of the information, public record or official record, or of 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 an individual's right to privacy 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 laws, 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; and

(c) Any employee or official 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 regulations.

SECTION 8. People's Freedom of 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 information:

(a) The location and contact information of the head, regional, provincial, and field offices, and other established places where the public can submit requests to obtain information;
(b) The person or officer responsible for receiving requests for information;
(c) The procedure for the filing and processing of the request, as provided in the succeeding Section 9 of this Order;
(d) The standard forms for the submission of requests and for the proper acknowledgment of such requests;
(e) The process for the disposition of requests;
(f) The procedure for administrative appeal of any denial of request for access to information; and
(g) The schedule of applicable fees.

SECTION 9. Procedure. The following procedure shall govern the filing and processing of requests 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 of exceptions as hereinabove provided.

(b) The public official receiving the request shall provide reasonable assistance, free of charge, to enable all requesting parties, 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 or 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 the 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 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 events or other analogous cases. The government office shall

notify the person making the request of such extension, setting forth the reasons for the extension. In no case shall the extension go beyond twenty (20) working days counted from the end of the original period, 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 requested, 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 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 wholly or partially, it shall, as soon as practicable and within fifteen (15) working days from the receipt of the request, 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 for access to information.

SECTION 13. Remedies in Case of Denial of Request for Access to Information. A person whose request for access to information has been denied may avail himself of the remedies set forth below:

(a) Denial of any request for access to information may be appealed to the person or office next higher in authority, following the procedure mentioned in Section 8 (f) 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 shall 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 party may file the appropriate judicial action 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 and 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.

By the President:

SALVADOR C. MEDIALDEA
Executive Secretary

REPUBLIC OF THE PHILIPPINES
PRRD 2016 - 000156

CERTIFIED COPY:

MARIANITO M. DIMAANDAL
DIRECTOR IV
MALACAÑANG RECORDS OFFICE

7-25-2016

Office of the President
of the Philippines
Malacañang

MEMORANDUM FROM THE EXECUTIVE SECRETARY

TO: All Heads of Departments, Bureaus and Agencies of the National/Local Governments Including Government-Owned and Controlled Corporations (GOCCs), Government Financial Institutions (GFIs), and All Others Concerned

SUBJECT: **INVENTORY OF EXCEPTIONS TO EXECUTIVE ORDER NO. 2 (S. 2016)**

DATE: 24 November 2016

Pursuant to Section 4 of Executive Order (EO) No. 2 (s. 2016), the Office of the President hereby circularizes the inventory of exceptions to the right to access of information, for the guidance of all government offices and instrumentalities covered by EO No. 2 (s. 2016) and the general public.

The foregoing list of exceptions shall be without prejudice to existing laws, jurisprudence, rules or regulations authorizing the disclosure of the excepted information upon satisfaction of certain conditions in certain cases, such as the consent of the concerned party or as may be ordered by the courts.

In evaluating requests for information, all heads of offices are enjoined to ensure the meaningful exercise of the public of their right to access to information on public concerns.

For your information and guidance.

SALVADOR C. MEDIALDEA

CERTIFIED COPY:

MARIANITO M. DIMAANDAL
DIRECTOR IV
MALACAÑANG RECORDS OFFICE

Exceptions to Right of Access to Information

For the guidance of all government offices and instrumentalities covered by EO No. 2 (s. 2016) and the general public, the following are the exceptions to the right of access to information, as recognized by the Constitution, existing laws, or jurisprudence:[1]

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.

---

[1] 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.

For the implementation of the exceptions to the right of access to information, the following provide the salient details and legal bases that define the extent and application of the exceptions.

1. Information covered by Executive privilege:

   a. Presidential conversations, correspondences, and discussions in closed-door Cabinet meetings;[2] and

   b. Matters covered by deliberative process privilege, namely:

      i. advisory opinions, recommendations and deliberations comprising part of a process by which governmental decisions and policies are formulated; intra-agency or inter-agency recommendations or communications during the stage when common assertions are still in the process of being formulated or are in the exploratory stage; or information pertaining to the decision-making of executive officials;[3] and
      ii. information, record or document comprising drafts of decisions, orders, rulings, policy decisions, memoranda, etc.;[4]

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

   a. Information, record, or document that must be kept secret in the interest of national defense or security;[5]

   b. Diplomatic negotiations and other information required to be kept secret in the conduct of foreign affairs;[6] and

---

[2] This exception may only be invoked by the President and his close advisors. The extent of the privilege is defined by applicable jurisprudence: *Senate v. Ermita*, G.R. No. 169777, 20 April 2006, 488 SCRA 1; *Neri v. Senate Committee on Accountability of Public Officers and Investigations*, G.R. No. 180643, 4 September 2008, 564 SCRA 152; *Akbayan v. Aquino*, G.R. No. 170516, 16 July 2008, 558 SCRA 468; and *Chavez v. PCGG*, G.R. No. 130716, 9 December 1998, 299 SCRA 744.

[3] *Akbayan v. Aquino, supra*; *Chavez v. NHA*, G.R. No. 164527, 15 August 2007; and *Chavez v. PCGG, supra*. The privilege of invoking this exception ends when the executive agency adopts a definite proposition (*Department of Foreign Affairs v. BCA International Corp.*, G.R. No. 210858, 20 July 2016).

[4] Section 3(d) Rule IV, *Rules Implementing the Code of Conduct and Ethical Standards for Public Officials and Employees* (Rules on CCESPOE). Drafts of decisions, orders, rulings, policy decisions, memoranda, and the like, such as resolutions prepared by the investigating prosecutor prior to approval for promulgation and release to parties [*Revised Manual for Prosecutors of the Department of Justice (DOJ)*] are also covered under this category of exceptions.

[5] *Almonte v. Vasquez*, G.R. No. 95367, 23 May 1995, 244 SCRA 286; *Chavez v. PCGG, supra; Legaspi v. Civil Service Commission*, L-72119, 29 May 1987, 150 SCRA 530; *Chavez v. NHA, supra; Neri v. Senate, supra; Chavez v. Public Estates Authority*, G.R. No. 133250, 9 July 2002, 384 SCRA 152; and Section 3(a), Rule IV, Rules on CCESPOE. This exception generally includes matters classified under Memorandum Circular (MC) No. 78, as amended by MC No. 196 as "Top Secret," "Secret," "Confidential," and "Restricted."

[6] *Akbayan v. Aquino, supra;* Section 3(a) Rule IV, Rules on CCESPOE. This privilege may be invoked by the Department of Foreign Affairs and other government bodies involved in diplomatic negotiations.

c. Patent applications, the publication of which would prejudice national security and interests;[7]

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

a. Investigation records compiled for law enforcement purposes or information which if written would be contained in such records, but only to the extent that the production of such records or information would –

i. interfere with enforcement proceedings;
ii. deprive a person of a right to a fair trial or an impartial adjudication;
iii. disclose the identity of a confidential source and in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source; or
iv. unjustifiably disclose investigative techniques and procedures;[8]

b. Informer's privilege or the privilege of the Government not to disclose the identity of a person or persons who furnish information of violations of law to officers charged with the enforcement of law;[9]

c. When disclosure of information would put the life and safety of an individual in imminent danger;[10]

d. Any information given by informants leading to the recovery of carnapped vehicles and apprehension of the persons charged with carnapping;[11] and

e. All proceedings involving application for admission into the Witness Protection Program and the action taken thereon;[12]

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

---

[7] The applicability of this exception is determined by the Director General of the Intellectual Property Office and subject to the approval of the Secretary of the Department of Trade and Industry. Section 44.3 of the *Intellectual Property Code* (RA No. 8293, as amended by RA No. 10372).

[8] Section 3(f), Rule IV, Rules on CCESPOE; *Chavez v. PCGG*, *supra*. May be invoked by law enforcement agencies.

[9] *Akbayan v. Aquino*, *supra*; and Section 51, *Human Security Act of 2007* (RA No. 9372). May be invoked by law enforcement agencies.

[10] Section 3(b), Rule IV, Rules on CCESPOE.

[11] Section 19, *New Anti Carnapping Act of 2016* (RA No. 10883). May be invoked by law enforcement agencies.

[12] Section 7, *Witness Protection, Security and Benefit Act* (RA No. 6981).

a. Information of a personal nature where disclosure would constitute a clearly unwarranted invasion of personal privacy,[13] personal information or records,[14] including sensitive personal information, birth records,[15] school records,[16] or medical or health records;[17]

Sensitive personal information as defined under the *Data Privacy Act of 2012* refers to personal information:[18]

(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.

However, personal information may be disclosed to the extent that the requested information is shown to be a matter of public concern or interest, shall not meddle with or disturb the private life or family relations of the individual[19] and is not prohibited by any law or regulation. Any disclosure of personal information shall be in accordance with the principles of transparency, legitimate purpose and proportionality.[20]

Disclosure of personal information about any individual who is or was an officer or employee of a government institution shall be allowed, provided that such information relates to the position or functions of the individual, including: (1) the fact that the individual is or was an officer or employee of

---

[13] Section 3(e), Rule IV, Rules on CCESPOE.

[14] Sections 8 and 15, *Data Privacy Act of 2012* (RA No. 10173); *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 [Section 3(g), *Data Privacy Act of 2012*]; Article 26, Civil Code. May be invoked by National Privacy Commission and government personal information controllers.

[15] Article 7, *The Child and Youth Welfare Code* [Presidential Decree (PD) No. 603].

[16] Section 9(4), *Education Act of 1982* [Batas Pambansa (BP) Blg. 232].

[17] Medical and health records are considered as sensitive personal information pursuant to Section 3(l)(2), *Data Privacy Act of 2012*; See also Department of Health-Department of Science and Technology (DOST)-Philippine Health Insurance Corporation Joint Administrative Order No. 2016-0002 (Privacy Guidelines for the Implementation of the Philippine Health Information Exchange).

[18] Section 3(l), *Data Privacy Act of 2012*.

[19] Article 26(2), *Civil Code*.

[20] Section 11, *Data Privacy Act of 2012*.

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;[21]

b. Source of any news report or information appearing in newspapers, magazines or periodicals of general circulation obtained in confidence;[22] and

c. Records of proceedings and processes deemed confidential by law for the privacy and/or protection of certain individuals, such as children, victims of crime, witnesses to a crime or rehabilitated drug offenders, including those pertaining to the following:

(1) records of child and family cases;[23]
(2) children in conflict with the law from initial contact until final disposition of the case;[24]
(3) a child who is a victim of any offense under the *Anti-Child Pornography Act of 2009*, including the name and personal circumstances of the child, or the child's immediate family, or any other information tending to establish the child's identity;[25]
(4) a child witness, who is a victim of a crime, an accused of a crime, or a witness to a crime, including the name, address, telephone number, school, or other identifying information of a child or an immediate family of the child;[26]
(5) cases involving violence against women and their children, including the name, address, telephone number, school, business, address, employer, or other identifying information of a victim or an immediate family member;[27]
(6) trafficked persons, including their names and personal circumstances, or any other information tending to establish the identity of the trafficked person;[28]
(7) names of victims of child abuse, exploitation or discrimination;[29]

---

[21] Section 4, *Data Privacy Act of 2012*.

[22] *An Act to Exempt the Publisher, Editor or Reporter of any Publication from Revealing the Source of Published News or Information Obtained in Confidence* (RA No. 53), as amended by RA No. 1477. May be invoked by government newspapers.

[23] Section 12, *Family Courts Act of 1997* (RA Act No. 8369).

[24] Section 43, *Juvenile Justice and Welfare Act of 2006* (RA No. 9344).

[25] Section 13, *Anti-Child Pornography Act of 2009* (RA No. 9775).

[26] Section 31, A.M. No. 00-4-07-SC, *Re: Proposed Rule on Examination of a Child Witness*.

[27] Section 44, *Anti-Violence Against Women and their Children Act of 2004* (RA No. 9262); and *People v. Cabalquinto*, G.R. No. 167693, 19 September 2006.

[28] Section 7, *Anti-Trafficking in Persons Act of 2003* (RA No. 9208), as amended by RA No. 10364.

[29] Section 29, *Special Protection of Children Against Abuse, Exploitation and Discrimination Act* (RA No. 7610).

(8) disclosure which would result in undue and sensationalized publicity of any case involving a child in conflict with the law, child abuse, or violation of anti-trafficking of persons;[30]

(9) records, documents and communications of proceedings involving domestic and inter-country adoptions, including the identity of the child, natural parents and adoptive parents;[31]

(10) names of students who committed acts of bullying or retaliation;[32]

(11) first time minor (drug) offenders under suspended sentence who comply with applicable rules and regulations of the Dangerous Drugs Board and who are subsequently discharged; judicial and medical records of drug dependents under the voluntary submission program; and records of a drug dependent who was rehabilitated and discharged from treatment and rehabilitation centers under the compulsory submission program, or who was charged for violation of Section 15 (use of dangerous drugs) of the *Comprehensive Dangerous Drugs Act of 2002*, as amended; and [33]

(12) identity, status and medical records of individuals with Human Immunodeficiency Virus (HIV), as well as results of HIV/Acquired Immune Deficiency Syndrome (AIDS) testing;[34]

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, such as but not limited to the following:

a. Trade secrets, intellectual property, business, commercial, financial and other proprietary information;[35]

---

[30] Section 14, *Juvenile Justice and Welfare Act of 2006*; Section 7, *Anti-Trafficking in Persons Act of 2003*, as amended; and Section 29, *Special Protection of Children Against Abuse, Exploitation and Discrimination Act*.

[31] Section 15, *Domestic Adoption Act of 1998* (RA No. 8552) and Section 43, IRR of RA No. 8552; Sections 6 and 16(b), *Inter-Country Adoption Act of 1995* (RA No. 8043) and Sections 53, 54 and 55 of IRR of RA No. 8043.

[32] Section 3(h), *Anti-Bullying Act* (RA No. 10627).

[33] Sections 60, 64 and 67, *Comprehensive Dangerous Drugs Act of 2002* (RA No. 9165).

[34] Sections 2(b), 18, 30, and 32, *Philippine AIDS Prevention and Control Act of 1998* (RA No. 8504).

[35] Sections 45, 106.1, and 150.2, *The Intellectual Property Code* (RA No. 8293, as amended by RA No. 10372); Section 66.2, *Securities Regulation Code* (RA No. 8799); DOST Administrative Order No. 004-16; Section 142, *The Corporation Code* (BP Blg. 68); Section 34, *Philippine Competition Act* (RA No. 10667); Sections 23 and 27 (c), *The New Central Bank Act* (RA No. 7653); *Anti-Money Laundering Act* (RA No. 9160); Section 18, *Strategic Trade Management Act* (RA No. 10697); Sections 10 and 14, *Safeguard Measures Act* (RA No. 8800); Section 12, *Toxic Substances and Hazardous and Nuclear Wastes Control Act of 1990* (RA No. 6969); Article 290, *Revised Penal Code*; Section 10.10, Rule 10, 2012 Revised IRR of *Build-Operate-Transfer Law* (RA No. 6957); and *Revised Philippine Ports Authority Manual of Corporate Governance*.

b. Data furnished to statistical inquiries, surveys and censuses of the Philippine Statistics Authority (PSA);[36]

c. Records and reports submitted to the Social Security System by the employer or member;[37]

d. Information gathered from HIV/AIDS contact tracing and all other related health intelligence activities;[38]

e. Confidential information submitted to the Philippine Competition Commission prohibited from disclosure by law, including the identity of the person who provided the information under condition of anonymity;[39]

f. Applications and supporting documents filed pursuant to the *Omnibus Investments Code of 1987*;[40]

g. Documents submitted through the Government Electronic Procurement System;[41]

h. Information obtained from accessing any electronic key, electronic data message, or electronic document, book, register, correspondence, information or other material pursuant to any powers conferred under the *Electronic Commerce Act of 2000*;[42]

i. Any confidential information supplied by the contractors in mineral agreements, and financial or technical assistance agreements pursuant to the *Philippine Mining Act of 1995* and its Implementing Rules and Regulations (IRR), during the term of the project to which it relates;[43]

j. Information received by the Department of Tourism (DOT) in relation to the accreditation of accommodation establishments (such as hotels and resorts) and travel and tour agencies;[44]

---

[36] Section 26, *Philippine Statistical Act of 2013* (RA No. 10625); and Section 4, *Commonwealth Act No. 591*. May be invoked only by the PSA.

[37] Section 24(c), *Social Security Act of 1997* (RA No. 1161, as amended by RA No. 8282).

[38] Section 29, *Philippine AIDS Prevention and Control Act of 1998* (RA No. 8504).

[39] Section 34, *Philippine Competition Act* (PCA), RA No. 10667 and Section 13, Rule 4 of the IRR of PCA. This exception can be invoked by the Philippine Competition Commission subject to well-defined limitations under the PCA.

[40] Section 81, EO No. 226 (s. 1987), as amended.

[41] Section 9, *Government Procurement Reform Act* (RA No. 9184).

[42] Section 32, *Electronic Commerce Act of 2000* (RA No. 8792).

[43] Section 94(f), *Philippine Mining Act of 1995* (RA No. 7942).

[44] Section 1, Rule IX, DOT MC No. 2010-02 (Rules and Regulations to Govern, the Accreditation of Accommodation Establishments – Hotels, Resorts and Apartment Hotels); and Section 23, DOT MC No. 2015-06 (Revised Rules and Regulations to Govern the Accreditation of Travel and Tour Agencies).

k. The fact that a covered transaction report to the Anti-Money Laundering Council (AMLC) has been made, the contents thereof, or any information in relation thereto;[45]

l. Information submitted to the Tariff Commission which is by nature confidential or submitted on a confidential basis;[46]

m. Certain information and reports submitted to the Insurance Commissioner pursuant to the *Insurance Code*;[47]

n. Information on registered cultural properties owned by private individuals;[48]

o. Data submitted by a higher education institution to the Commission on Higher Education (CHED);[49] and

p. Any secret, valuable or proprietary information of a confidential character known to a public officer, or secrets of private individuals;[50]

6. Information of which a premature disclosure would:

a. in the case of a department, office or agency which agency regulates currencies, securities, commodities, or financial institutions, be likely to lead to significant financial speculation in currencies, securities, or commodities, or significantly endanger the stability of any financial institution; or

b. be likely or significantly frustrate implementation of a proposed official action, except such department, office or agency has already disclosed to the public the content or nature of its proposed action, or where the department, office or agency is required by law to make such disclosure on its own initiative prior to taking final official action on such proposal.[51]

7. Records of proceedings or information from proceedings which, pursuant to law or relevant rules and regulations, are treated as confidential or privileged, including but not limited to the following:

---

[45] Section 9(c), *Anti-Money Laundering Act of 2001*, as amended. May be invoked by AMLC, government banks and its officers and employees.

[46] Section 10, *Safeguard Measures Act.*

[47] Section 297 in relation with Section 295 and Section 356, *The Insurance Code* (as amended by RA No. 10607).

[48] Section 14, *National Cultural Heritage Act of 2009* (RA No. 10066).

[49] CHED Memorandum Order No. 015-13, 28 May 2013.

[50] Articles 229 and 230, *Revised Penal Code*; Section 3(k), *Anti-Graft and Corrupt Practices Act* (RA No. 3019); Section 7(c), *Code of Conduct and Ethical Standards for Public Officials and Employees* (RA No. 6713); Section 7, *Exchange of Information on Tax Matters Act of 2009* (RA No. 10021); and Section 6.2, *Securities Regulation Code* (RA No. 8799).

[51] Section 3(g), Rule IV, Rules on CCESPOE.

a. Mediation and domestic or international arbitration proceedings, including records, evidence and the arbitral awards, pursuant to the *Alternative Dispute Resolution Act of 2004*;[52]

b. Matters involved in an Investor-State mediation;[53]

c. Information and statements made at conciliation proceedings under the *Labor Code*;[54]

d. Arbitration proceedings before the Construction Industry Arbitration Commission (CIAC);[55]

e. Results of examinations made by the Securities and Exchange Commission (SEC) on the operations, books and records of any corporation, and all interrogatories propounded by it and the answers thereto;[56]

f. Information related to investigations which are deemed confidential under the *Securities Regulations Code*;[57]

g. All proceedings prior to the issuance of a cease and desist order against pre-need companies by the Insurance Commission; [58]

h. Information related to the assignment of the cases to the reviewing prosecutors or the undersecretaries in cases involving violations of the *Comprehensive Dangerous Drugs Act of 2002*;[59]

i. Investigation report and the supervision history of a probationer;[60]

j. Those matters classified as confidential under the *Human Security Act of 2007*;[61]

---

[52] Sections 9, 23 and 33, *Alternative Dispute Resolution (ADR) Act of 2004* (RA No. 9285); and DOJ Circular No. 98 (s. 2009) or the IRR of the ADR Act.

[53] Article 10, International Bar Association Rules for Investor-State Mediation.

[54] Article 237, *Labor Code*.

[55] Section 7.1, Rule 7, CIAC Revised Rules of Procedure Governing Construction Arbitration.

[56] Section 142, *Corporation Code*. May be invoked by the SEC and any other official authorized by law to make such examination.

[57] Sections 13.4, 15.4, 29.2 (b), and 64.2 of the *Securities Regulation Code*.

[58] Section 53(b)(1) of the *Pre-Need Code of the Philippines*. The confidentiality of the proceedings is lifted after the issuance of the cease and desist order.

[59] DOJ Department Circular No. 006-16 (No. 6), 10 February 2016.

[60] Section 17, *Probation Law of 1976* [PD No. 968 (s.1976)].

[61] Sections 9, 13, 14, 29, 33 and 34, *Human Security Act of 2007* (RA No. 9372).

k. Preliminary investigation proceedings before the committee on decorum and investigation of government agencies;[62] and

l. Those information deemed confidential or privileged pursuant to pertinent rules and regulations issued by the Supreme Court, such as information on disbarment proceedings, DNA profiles and results, or those ordered by courts to be kept confidential;[63]

8. Matters considered confidential under banking and finance laws and their amendatory laws, such as:

a. RA No. 1405 (*Law on Secrecy of Bank Deposits*);

b. RA No. 6426 (*Foreign Currency Deposit Act of the Philippines*) and relevant regulations;

c. RA No. 8791 (*The General Banking Law of 2000*);

d. RA No. 9160 (*Anti-Money Laundering Act of 2001*); and

e. RA No. 9510 (*Credit Information System Act*);

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

a. Those deemed confidential pursuant to treaties, executive agreements, other international agreements, or international proceedings, such as:

(1) When the disclosure would prejudice legitimate commercial interest or competitive position of investor-states pursuant to investment agreements;[64]
(2) Those deemed confidential or protected information pursuant to United Nations Commission on International Trade Law Rules on Transparency in Treaty-based Investor-State Arbitration and Arbitration Rules (UNCITRAL Transparency Rules);[65] and
(3) Refugee proceedings and documents under the *1951 Convention Relating to the Status of Refugees*, as implemented by DOJ Circular No. 58 (s. 2012);

---

[62] Section 14, Civil Service Commission Resolution No. 01-0940.

[63] Section 18, Rule 139-B and Section 24, Rule 130 of the Rules of Court; and Section 11 of the Rule on DNA Evidence, A.M. No. 06-11-5-SC.

[64] Examples: Article 20 (2), ASEAN Comprehensive Investment Agreement; Article 15 (2) Agreement on Investment under the Framework Agreement on the Comprehensive Economic Cooperation between the ASEAN and the Republic of India; and Article 15 (2) of the Agreement on Investment under the Framework Agreement on the Comprehensive Economic Cooperation among the Government of the Member Countries of the ASEAN and the Republic of Korea.

[65] Article 7, UNCITRAL Transparency Rules.

b. Testimony from a government official, unless pursuant to a court or legal order;[66]

c. When the purpose for the request of Statement of Assets, Liabilities and Net Worth is any of the following:

   (1) any purpose contrary to morals or public policy; or
   (2) any commercial purpose other than by news and communications media for dissemination to the general public;[67]

d. Lists, abstracts, summaries of information requested when such lists, abstracts or summaries are not part of the duties of the government office requested;[68]

e. Those information and proceedings deemed confidential under rules and regulations issued by relevant government agencies or as decided by the courts;[69]

f. Requested information pertains to comments and disclosures on pending cases in judicial proceedings;[70] and

g. Attorney-client privilege existing between government lawyers and their client.[71]

---

[66] *Senate v. Neri*, *supra*; *Senate v. Ermita*, *supra*.

[67] Section 8(D), *Code of Conduct and Ethical Standards for Public Officials and Employees*.

[68] *Belgica v. Ochoa*, G.R. No. 208566, 19 November 2013; and *Valmonte v. Belmonte Jr.*, G.R. No. 74930, 13 February 1989, 252 Phil. 264.

[69] Examples: 2012 Guidelines and Procedures in the Investigation and Monitoring of Human Rights Violations and Abuses and the Provision of CHR Assistance; Government Service Insurance System's Rules of Procedure of the Committee on Claims; National Labor Relations Commission Resolution No. 01-02, Amending Certain Provisions of the New Rules of Procedure of the National Labor Relations Commission, 08 March 2002; Department of Agrarian Reform MC No. 07-11, 19 July 2011; Department of Social Welfare and Development MC No. 021-12, 16 October 2012; and Section 42, *Investment Company Act* (RA No. 2629); When the information requested is not a matter of public concern or interest as decided in *Hilado v. Judge Amor A. Reyes*, G.R. No. 163155, 21 July 2006.

[70] *Romero v. Guerzon*, G.R. No. 211816, 18 March 2015.

[71] Canon 21 of the *Code of Professional Responsibility*.

OFFICE OF THE PRESIDENT
OF THE PHILIPPINES

MEMORANDUM CIRCULAR NO. 78

PROMULGATING RULES GOVERNING SECURITY OF CLASSIFIED MATTER IN GOVERNMENT OFFICES.

The following regulations entitled "SECURITY OF CLASSIFIED MATTER IN GOVERNMENT DEPARTMENTS AND INSTRUMENTALITIES" for safeguarding official matters affecting the national security, to be enforced and observed in all departments, bureaus, offices and agencies of the government in all national, provincial, municipal and city levels, are hereby promulgated:

SECURITY OF CLASSIFIED MATTER IN
GOVERNMENT DEPARTMENTS & INSTRUMENTALITIES

Section I

GENERAL

1. Classification categories. -

a. Official matter which requires protection in the interest of national security shall be limited to four categories of classification which, in descending order of importance, shall carry one of the following designations:

(1) TOP SECRET
(2) SECRET
(3) CONFIDENTIAL
(4) RESTRICTED

b. The classifications mentioned in sub-paragraph a above shall not be attached to a matter which does not involve the national security or which does not relate to any one of those specifically enumerated in paragraphs 4, 11, 17, and 23, below.

2. Definition of terms. -

a. The term "Department" is used to cover any Philippine Government Department, Service, or Instrumentality.

b. The term "matter" includes everything, regardless of its physical character, on or in which information is recorded or embodied. Documents, equipment, projects, books, reports, articles, notes, letters, drawings, sketches, plans, photographs, recordings, machinery, models, apparatus, devices, and all other products or substances fall within the general term "matter". Information which is transmitted orally is considered as "matter" for purposes of security.

c. The term "officer" includes any Government or Armed Forces official of officer permanently or temporarily employed in a Department as defined in a.

d. The term "document" covers any form of recorded information, including printed, written, drawn or painted matter, sound recordings, photographs, films, etc. "Documents" are included in "matter"

e. The term "equipment" includes machinery, apparatus, devices, supplies, ammunition, etc.

f. "Security Clearance" is the certification by a responsible authority that the person described is cleared for access to classified matter at the appropriate level.

write 2

g. The term "need to know" is the principle whereby access to classified matter may only be given to those persons to whom it necessary for the fulfillment of their duties. Persons are not e to have access to classified matter solely by virtue of their stat

h. The term "custodian" is an individual who has possession of or is otherwise charged with the responsibility for safeguarding and accounting of classified material.

i. "Certificate of Destruction" is the certification by a witnessing officer that the classified matter described therein has been disposed of, in his presence, by approved destruction methods (ANNEX A).

j. The term "physical security" is the safeguarding by physical means, such as guards, fire protection measures and other similar means, of information, personnel, property, utilities, facilities and installations against compromise, trespass, sabotage, pilferage, theft, espionage or any other dishonest or criminal act.

3. Security Officers. - A properly trained and cleared Security Officer shall be appointed in every Department of the Government which handles classified matter. He shall undergo training to be conducted by the National Intelligence Coordinating Agency or Armed Forces of the Philippines intelligence agencies. He shall be responsible to the Head of the Department for the implementation and enforcement of these regulations and the necessary action on breaches of security. Before appointment as a Security Officer, an officer must first be cleared by the Head of the Department for access to the highest classified matter the Department is authorized to handle. In providing this clearance, the Head of the Department may coordinate with the National Intelligence Coordinating Agency or the Department of National Defense.

Section II

TOP SECRET MATTER

4. Definition. - Information and material (matter) the unauthorized disclosure of which would cause exceptionally grave damage to the nation, politically, economically, or from a security aspect. This category is reserved for the nation's closest secrets and is to be used with great reserve.

Examples:

a. Very important political documents dealing with such matters as negotiations for major alliances.

b. Major governmental projects such as drastic proposals to adjust the nation's economy (before official publication).

c. Matter relating to new and far reaching experimental, technical and scientific developments in methods of warfare or defense, e.g., vital matter relating to atomic warfare, defense against biological warfare, or matter affecting future operational strategy. A TOP SECRET grading is justified if:

(1) It is likely to influence military strategy materially;

(2) It gives us a prolonged military advantage over other nations;

(3) It is liable to compromise some other project similarly graded.

d. Critical information relating to vital strategic areas and the supply of vital strategic materials.

e. Information which would indicate the capabilities or major successes of our intelligence services or which would imperil secret sources.

f. Critical information about cryptography in so far as it relates to devices and equipment under development.

g. Certain compilations of data or items which individually may be classified SECRET or lower, but which collectively should be put in a higher grade.

5. Classification Authority. -

a. Original classification authority for assignment of TOP SECRET classification rests exclusively with the Head of the Department. This power may, however, be delegated to authorized officers in instances when the necessity for such arises.

b. Derivative classification authority for TOP SECRET classification may be granted those officers who are required to give comments or responses to a communication that necessitates TOP SECRET response.

6. Reproduction. -

a. TOP SECRET matter may be copied, extracted, or reproduced only when the classifying authority has authorized such action. Permission to reproduce shall not extend beyond a specified number of copies which are to be accorded the same treatment as the original. At the time of issuance of any TOP SECRET document, the classifying authority shall insure that each copy of the document contains a notation substantially as follows:

(1) "Reproduction of this document in whole or in part is prohibited except with the permission of the issuing office or higher authority;" or

(2) "Reproduction of paragraph(s) _____ of this document is prohibited except with the permission of the issuing office or higher authority; other paragraphs may be reproduced."

b. The reproduction of TOP SECRET matter shall be carried out under the supervision of an authorized officer. All materials and waste incidental to the reproduction shall be accounted for and disposed of as prescribed in sub-paragraph 10a below.

7. Inventory. - The Head of the Department shall require physical inventory of all TOP SECRET matter in the custody of his Department at least once a year. Appropriate action on custodial deficiencies shall be made.

8. Transmission. -

a. TOP SECRET matter in the clear shall be transmitted

by any of the following means:

(1) By direct contact of officers concerned.

(2) By the officially designated courier.

(3) By accompanied Department of Foreign Affairs diplomatic pouch.

b. TOP SECRET matter shall not be transmitted by mail, express or electrical means, unless in cryptographic form.

9. Storage. - TOP SECRET matter shall be stored -

a. In a safe, steel file cabinet or other steel container equipped with a built-in, three-position, dial-type combination lock which is of such weight, size and construction as to minimize possibility of physical theft or damage by fire or tampering.

b. In a secure room or vault which is approved for such use by the Head concerned and which assures protection comparable to sub-paragraph a above.

10. Destruction. - TOP SECRET matter, which becomes eligible for destruction in accordance with approved schedules, shall be destroyed as prescribed below:

a. Destruction shall be accomplished by burning or pulping by the custodian in the presence of a witnessing officer designated by the responsible Head. Witnessing personnel must have a TOP SECRET clearance.

b. A certificate of destruction shall be prepared and forwarded to the originating office.

Section III

SECRET MATTER

11. Definition. - Information and material (matter) the unauthorized disclosure of which would endanger national security, cause serious injury to the interest or prestige of the nation or of any governmental activity or would be of great advantage to a foreign nation.

Examples:

a. High level directives dealing with important negotiations (as distinct from major negotiations which would be in the TOP SECRET category) with other countries.

b. Proposals for new schemes of governmental or other controls, foreknowledge of which would seriously prejudice their operation.

c. Matter relating to certain new methods of warfare or defence, including scientific and technical developments, not classified as TOP SECRET, e.g., new designs of Service aircraft, guided projectiles, tanks, radar and anti-submarine devices. A SECRET grading is justified if:

(1) It materially influences a major aspect of military tactics;

(2) It involves a novel principle applicable to existing important projects;

(3) It is sufficiently revolutionary to result in a major advance in existing techniques or in the performance of existing secret weapons;

(4) It is liable to compromise some other projects already so graded.

d. Plans or details of schemes for the defense of areas other than vital strategic areas, including plans or particulars of operations connected with them.

e. Vital military information, including photographs, maps, etc., relating to important defenses, establishments, and installations.

f. Intelligence which is not in the TOP SECRET category but which would reveal a secret source, or the value of which depends upon concealing the fact that we possess it.

g. Cryptographic devices and equipment unless specifically assigned to a lower classification.

h. Certain compilations of data or items which individually may be classified CONFIDENTIAL or lower, but which collectively should be put in a higher grade.

12. Classification Authority. - Same as for TOP SECRET matter.

13. Reproduction. - Same as for TOP SECRET matter.

14. Transmission - SECRET matter shall be transmitted as indicated below:

a. Between points within the Philippines:

(1. Direct contact of officers concerned.

(2) Electrical means in cryptographic form.

(3) Courier specifically authorized by the transmitting agency.

(4) Philippine registered mail.

b. Between points from within and outside the Philippines and vice-versa, and between points outside the Philippines:

(1) As authorized in sub-paragraphs 14a(1) through (3) above.

(2) Accompanied Department of Foreign Affairs diplomatic pouch.

15. Storage. - SECRET matter shall be stored in a manner authorized for TOP SECRET documents, or in metal file cabinets equipped with a steel lockbar and combination padlock of which the manufacturer's identification numbers have been obliterated. The file cabinets must be of such size, weight, construction or installation so as to minimize the chance of unauthorized physical removal or the possibility of persons gaining

unauthorized access by transferring or manipulation or damage by fire.

16. Destruction. - Same as for TOP SECRET matter except that the witnessing officer need have SECRET clearance only and that no certificate of destruction need be prepared. Only records of destruction shall be maintained.

Section IV

CONFIDENTIAL MATTER

17. Definition. - Information and material (matter) the unauthorized disclosure of which, while not endangering the National Security, would be prejudicial to the interest or prestige of the nation or any government activity, or would cause administrative embarrassment or unwarranted injury to an individual or would be of advantage to a foreign nation.

Examples:

a. Plans of Government projects such as land development, hydro-electric schemes, road development, or development of areas.

b. Routine Service reports, e.g., on operations and exercises, which contain information of value but not of vital interest to a foreign power.

c. Routine Intelligence reports.

d. Technical matter not of major importance but which has a distinct military value or requires protection otherwise, e.g., new weapons calculated to influence minor tactics or Service tests of war equipment of a standard pattern. A CONFIDENTIAL grading is justified if:

(1) It is more than a routine modification or logical improvement of existing materials and is sufficiently advanced to result in substantial improvement in the performance of existing CONFIDENTIAL weapons;

(2) It is sufficiently important potentially to make it desirable to postpone knowledge of its value reaching a foreign nation;

(3) It is liable to compromise some other project already so graded.

e. Certain personnel records and staff matters.

f. Certain compilations of data or items which individually may be classified RESTRICTED, or which may be unclassified, but the aggregation of which enhances their security value.

g. Matters, investigations and documents of a personal and disciplinary nature, the knowledge of which is desirable to safeguard for administrative reasons.

h. Identification of personnel being investigated for misconduct, anomaly or fraud prior to the filing of appropriate charges or completion of the findings of boards created for such purpose.

18. Classification Authority. - Any officer is authorized to assign CONFIDENTIAL classification to any matter in the performance of his duties.

19. Reproduction. - The copying, extracting from or reproduction of CONFIDENTIAL matter is authorized except when the originator or higher authority has specifically denied this authority.

20. Transmission. - Same as for SECRET matter.

21. Storage. - Same as for SECRET matter.

22. Destruction. - Same as for SECRET matter except that the presence of a witnessing officer and records of destruction are not required.

Section V

RESTRICTED MATTER

23. Definition. - Information and material (matter) which requires special protection other than that determined to be TOP SECRET, SECRET or CONFIDENTIAL.

Examples:

a. Departmental books of instruction and training and technical documents intended for official use only or not intended for release to the public.

b. Routine information relating to the supply and procurement of military stores.

c. Minor modifications and routine tests of equipment.

d. Certain compilations of data or items which individually may be reclassified but which in the aggregate warrant a classification.

24. Authority to Classify, Reproduction, Dissemination, and Destruction. - Authority to classify shall be the same as for CONFIDENTIAL matter. Reproduction is authorized. Transmission shall be through the normal dissemination system. Destruction shall be the same as for that of CONFIDENTIAL matter.

Section VI

CLASSIFYING AND MARKING

25. General. - The originators of classified matter shall be responsible for its proper classification. Overclassification should be avoided because it prejudices the integrity of the classification system, depreciates the importance of correctly classified matter and creates unnecessary delay, expense and administrative burden.

26. Rules for classification. -

a. Documents shall be classified according to their content.

b. The overall classification of a file or a group of physically connected documents shall be at least as high as that of the highest classified document therein. Pages, paragraphs, sections or components thereof may bear different classifications. Documents separated from the file or group shall be handled in accordance with their individual classifications.

c. Transmittal documents or indorsements which do not contain classified information or which contain information classified lower than that of the preceding element or inclosure shall include a notation for automatic downgrading.

d. Correspondence, indices, receipts, reports of possession, transfer or destruction, catalogs or accession lists shall not be classified if any reference to classified matter does not disclose classified information.

e. Classified matter obtained from other Departments shall retain the same original classification.

f. Classified matter furnished to the Philippine Government by a foreign government or international organization shall be assigned a classification which will assure a degree of protection equivalent to that required by the government or international organization which furnished the classified matter. In addition, any special handling instruction shall be complied with.

27. Classification marking. - Classified matter shall be marked as follows:

a. Unbound documents. - The assigned classification for unbound documents, such as letters, memoranda, reports, telegrams and similar documents, the pages of which are not permanently and securely fastened together, shall be marked or stamped (not typed) conspicuously at the top and bottom of all pages which contain classified information. In marking, stamping, or printing the classification categories, the letters shall be larger than the normal lettering of the rest of the document. Front and back covers, and title pages, when used; first pages; and any routing instructions or other papers of any size which conceal or partially conceal the cover, the title or first page shall bear the marking of the overall classification of the document. Other pages, except pages of messages to be transmitted electrically, shall be marked according to the classification of their own content. A cover shall be marked on its outer surface.

b. Permanently bound documents. - A permanently bound document is defined as one from which the pages cannot be removed without damage or mutilation. The classification of permanently bound documents, such as books or pamphlets shall be conspicuously marked, stamped or printed in letters larger than the normal lettering of the rest of the cover or page, at the top and bottom, on the first and back pages, and on the outside of the back cover.

c. Paragraphs, chapters, or sections. - The classification of a paragraph, chapter or section shall be indicated by including the initial of the appropriate classification in parenthesis at the end of such paragraph, chapter or section. Unclassified parts of classified documents will be marked "(U)".

d. Reproduction. - All copies or reproduction of classified matter shall be marked in the same manner as the original.

e. Photographs, films, and recordings. -

(1) Photographs - Negatives shall be marked with the appropriate classification markings and kept in containers bearing conspicuous classification markings. Roll negatives shall be marked at the beginning and end of each strip. Single negatives shall be marked with the appropriate classification. The top and bottom of each photographic print and the center of the reverse side shall be marked with the appropriate classification.

(2) Motion picture films - Classified motion picture films shall be marked at the beginning and end of each roll and in the title of each film, and shall be kept in containers bearing conspicuous classification markings.

(3) Sound recordings - Classified sound recordings shall be marked on readily observable portions with the appropriate markings, preferably at the beginning and at the end; when stored, the container shall display similar markings. When possible the classification shall be announced at the beginning and end of recordings.

f. Charts, maps, and drawings.- Classified charts, maps and drawings shall carry the classification marking under the legend, title block, or scale in such a manner that it can be reproduced on all copies made therefrom. Such classification shall also be prominently marked at the top and bottom in each instance and, if the document is rolled or folded, on the back in a clearly visible place.

g. Products or substances. - The assigned classification shall be conspicuously marked on classified products or substances and on their containers, if possible. If the article or container cannot be marked or if it is necessary to conceal the classified nature of the material, written notification of the classification shall be furnished the recipients of such products or substances.

h. Unclassified material. - Unclassified material should not be marked UNCLASSIFIED, unless it is essential to convey to a recipient of such material that it has been examined specifically with the view of imposing a classification and that it has been determined to be unclassified.

i. Material disseminated outside the Department. - When classified information is furnished to authorized persons outside the Department, the following notation, in addition to the assigned classification markings, shall be placed on the document, on the material, on its container, or, when as indicated in sub-paragraph g above, marking is impracticable, on the written notification of its assigned classification:

> "This material contains information affecting the national security of the Philippines, the transmission or revelation of which in any manner to unauthorized persons is punishable under the Revised Penal Code and the Espionage Act (CA Nr 616)."

28. Additional Markings. -

a. All pages of unbound TOP SECRET and SECRET documents shall be marked with the following: (COPY _____ OF _____ COPIES)
(PAGE _____ OF _____ PAGES)

b. All bound TOP SECRET and SECRET matter shall be marked on the front cover as follows: (COPY ____ OF ____ COPIES)

Section VII

CONTROL OF CLASSIFIED MATTER

29. Custody and accounting of classified matter. - Heads of Departments handling classified matter shall issue orders designating their respective custodians of classified matter. Custodians shall -

a. Store all classified matter.

b. Maintain a registry of classified matter showing all classified matter received and to whom transmitted.

c. Maintain a current roster of persons authorized access to classified matter for each classification in the office.

d. Insure physical security for classified matter.

e. Conduct an inventory of all TOP SECRET matter as specified in paragraph 7.

f. Upon his relief, account for all TOP SECRET and SECRET matter by inventory and transmit the same to his successor.

30. Unauthorized keeping of private records. - All government personnel are prohibited from keeping private records, diaries, or papers containing statements of facts or opinions, either official or personal, concerning matters which are related to or which affect national interest or security. Also prohibited are the collection of souvenirs or obtaining for personal use whatsoever any matter classified in the interest of national security.

31. Dissemination. - Dissemination of classified matter shall be restricted to properly cleared persons whose official duties require knowledge or possession thereof. Responsibility for the determination of "need-to-know" rests upon both each individual, who has possession, knowledge or command control of the information involved, and the recipient.

32. Discussion involving classified matter. -

a. Indiscreet discussions or conversation involving classified matter shall not be engaged in within the presence of or with unauthorized persons.

b. When a lecture, address or informal talk to a group includes classified matter, the speaker shall announce the classification at the beginning and end of the period.

e. All personnel leaving the Government Service shall be warned against unlawful disclosures of classified matter.

33. Disclosure to other Departments of classified information originating from another Department. - Classified matter originating from another Department shall not be disseminated to other Departments without the consent of the originating Department.

34. Release of classified matter outside a Department. -

a. General Policy. - No person in the Government shall convey orally, visually or by written communication any classified matter outside his own Department unless such disclosure has been processed and cleared by the Department Head or his authorized representative.

b. Release of classified matter to Congress. -

(1) Government personnel, when giving oral testimony before Congressional Committees involving classified matter, shall advise the committee of the classification thereof. Government personnel called upon to testify shall obtain necessary and prior instruction from his Department Head concerning disclosure.

(2) When Congressional members visit Government offices, Department Heads are authorized to release classified matter which is deemed an adequate response to an inquiry provided that it is required in the performance of official functions.

c. Disclosure to foreign governments or nationals. - Classified matter may be released to foreign governments or nationals of countries having defense obligations with the Philippines, in accordance with sub-paragraph 34a above. The release shall be made only after assurance by the requesting foreign agency or national that:

(1) Its use shall be solely for the purpose for which the classified matter is requested.

(2) It shall be treated or handled in accordance with the classification categories of the originating office.

(3) Handling shall be made by security-cleared personnel.

(4) Reproduction and dissemination shall not be made without the consent of the Department Head.

d. Disclosure of classified matter for publication. - Classified matter shall be released for public consumption only upon the consent of the Department Head or his authorized representative. However, in instances where there is a demand or need for releasing classified information, extreme care and caution must be exercised to analyze in detail the contents of the classified matter before release. Normally, all information are released through Public Information Officers. Public Information Officers should be assisted in the analysis of classified information by the Security Officer.

e. Disclosure through conferences and meetings. -

(1) Disclosure of classified matter in conferences

and other gatherings which include personnel outside the Department shall be in accordance with sub-paragraph 34a above. In conducting conferences involving classified information, the following data should be requested from each participant:

(a) Name and designation or position of participant.

(b) Address of participant.

(c) Signature of participant.

(2) Physical security of the conference room should be assured. Sponsoring agencies shall observe, among other things, the following:

(a) Arrangements for admission of those persons authorized to attend. All individuals must produce positive identification.

(b) Arrangements for protection of classified matter handled during the meeting.

(c) Control of signal equipment, notes and memoranda.

(d) Provision of adequate guards.

35. Removal of classified matter from offices for official use. -

a. Classified matter shall not be removed from offices for the purpose of working on such matter at night or for other purposes involving personal convenience. When necessity requires such removal, Department Heads through the Security Officer shall insure that adequate controls are established as follows:

(1) An appropriate authority specifically designated by the Department Head shall authorize each removal only after insuring that adequate security for the material can be provided.

(2) Storage safeguards shall be strictly observed.

b. Department Heads shall maintain a temporary record in whatever appropriate form of all classified matter removed from their facilities or installations to insure that they are accounted for.

36. Compromise or loss of classified matter. -

a. Any person who becomes aware of the disclosure, or the possibility of disclosure, of classified matter to any unauthorized person, or the loss of a classified document, shall immediately notify by the fastest means available the:

(1) Security Officer of the Department having primary interest (normally the originator), and the

(2) Department Head of the individual having custody.

b. The Department Head of the individual having custody shall cause an investigation to be made. This

investigation will fix individual responsibility for the compromise or possible compromise of TOP SECRET and SECRET matter and, when it can not be established, will fix responsibility on the appropriate officer who allowed the existence of inadequate or insecure conditions, which led to the compromise or possible compromise. In every case, the Head of the Department concerned shall take positive action to correct deficiencies and prevent recurrences, including appropriate disciplinary action and/or criminal prosecution against responsible individuals.

Section VIII

REGRADING AND DECLASSIFICATION

37. Responsibility for regrading. -

a. Each Department Head shall keep under continuing review all classified information in his custody, or of primary interest to him, and will initiate downgrading or declassifying action as soon as conditions warrant.

b. In obvious cases of overclassification or underclassification, higher authority may adjust the classification without referral to the originator, except to notify the originator of the change of classification. The originator will then take the action specified in paragraph 40.

38. Downgrading or declassification. -

a. Originators or letters of transmittal or other covering documents, classified solely or partially because of classified inclosures, shall place on such documents a notation substantially as follows:

"REGRADED UNCLASSIFIED (or appropriate classification) WHEN SEPARATED FROM CLASSIFIED INCLOSURES."

b. For classification purposes, indorsements and numbered comments or routing slips will be handled as separate documents.

c. Holders of classified matter may downgrade or declassify them when circumstances do not warrant retention in the original classification, provided the consent of the appropriate classification authority has been obtained. The downgrading or declassification of extracts from or paraphrases of classified documents also require the consent of the appropriate classification authority. Material which has been classified by a friendly foreign nation or international organization or another Department of the Philippine Government will be downgraded or declassified only with the consent of the originator.

39. Regrading. - If the recipient of classified matter believes that it has been classified too highly, he may request the originator for its downgrading or declassification. If the recipient of unclassified material believes that it should be classified or if the recipient of classified material believes that its classification is not sufficiently protective, the recipient may request the originator to classify the material or upgrade it.

40. Notification of change of classification. -

a. The official taking action to declassify, downgrade or upgrade classified material shall notify all addressees to whom the material was originally transmitted. Officials providing additional distribution (other than initial) of classified material should notify all recipients to whom the additional distribution was furnished of the regrading action required.

b. When downgrading a document in part, the originating Department shall notify recipients as to the new classification of separate chapters, sections, paragraphs or other appropriate subdivisions.

41. Marking of regraded documents. -

a. Authority annotation - Whenever classified matter is declassified, downgraded or upgraded, each copy of the material shall be marked or stamped on the front cover or on the first page, if the document has no cover, with a notice in the following manner:

(1) REGRADED _____ (enter new classification), BY AUTHORITY OF _____ (enter title or position of official authorized to make the change), BY _____ (enter name, grade and organization of the official making the change), ON _____ (enter the date on which the change was made).

b. Classification markings - Regraded documents and material shall be re-stamped or re-marked (not typed) as prescribed in paragraph 27 above and the old classification markings lined through. If the document is declassified, the classification markings on the outside of the front and back covers, title page and first and back pages of the text should be lined through. Prints of motion picture films shall show regrading or declassification action on leaders attached between the plain leader and first title frame.

c. Documents on file - When classified documents on file can not be immediately regraded for obvious reasons, such as the inability to screen a large volume of files to locate the document, the Department Head concerned may establish a system in which individual documents are regraded when charged out of the file for use or screened for regrading purposes, whichever occurs first. In cases requiring upgrading, material shall be given storage safeguards required by the new classification.

Section IX

TRANSMISSION OF CLASSIFIED MATTER

42. Classified document receipts. -

a. Transmission of TOP SECRET and SECRET documents shall be covered by a receipt system (ANNEX B). Transmission of CONFIDENTIAL documents may be covered by a receipt system when required by the sender.

b. The receipt form will identify the addressor, addressees and the document, but should not contain classified

information. It shall be signed by the recipient and returned to the sender. The name of the recipient shall be printed, stamped or typed on the form.

43. Cover Sheets. - Classified documents shall be covered with cover sheets as follows:

For TOP SECRET (ANNEX C)	- 8" x 13" white paper lined with 1/2" green border.
For SECRET (ANNEX D)	- 8" x 13" white paper lined with 1/2" red border.
For CONFIDENTIAL (ANNEX E)	- 8" x 13" white paper lined with 1/2" blue border.

Security classification and instructions are printed on the front page of the cover sheet. The back page is designed to show a record of transmission of the document it will cover.

a. All classified documents (CONFIDENTIAL and up), from the moment they are initiated, shall be covered by appropriate cover sheets, which shall stay with such documents until both are authorized for destruction.

b. When a TOP SECRET or SECRET document is reproduced, the reproduced copies shall be provided with new cover sheets and the "Record of Transmission" on the back page shall record only those personnel who handled each copy from the moment of its reproduction.

c. Cover sheets prescribed by this Executive Order shall be used only for classified documents transmitted among the various Departments of the National Government.

44. Preparation of classified matter for transmission outside a Department. -

a. Classified documents for transmission by Philippine registered mail or diplomatic pouch shall be prepared as follows:

(1) The documents shall be inclosed in two opaque envelopes or covers.

(2) A receipt shall be inclosed with the document as appropriate.

(3) The inner envelope or cover shall be addressed and sealed with sealing wax. The return adress should likewise be written in the inner envelope.

(4) The classification on the front and back of the inner envelope shall be marked in such a way that the markings will be easily seen when the outer cover is removed. Special markings required shall be placed on the front of the inner envelope.

(5) The inner envelope shall be inclosed in the opaque outer envelope or cover. The classification marking of the inner envelope must not be detectable through the outer envelope.

(6) The outer envelope with the inner envelope will then be forwarded. Classification or other special markings shall not appear on the outer envelope.

b. Classified documents for transmission through specifically authorized couriers shall be prepared as follows:

(1) The documents shall be inclosed in an opaque sealed envelope.

(2) The document shall be covered by a receipt as appropriate.

(3) The envelope shall be addressed and provided with a return address. No classification or other markings shall appear on the envelope.

45. Transmission within a Department. - Preparation of classified matter for transmission within a Department shall be governed by regulations issued by the Head of the Department.

Section X

SECURITY OF CONTAINERS

46. Unlocked containers. -

a. Any person finding a container of classified matter unlocked and unattended shall:

(1) Report such fact immediately to the Head of the Department concerned, or to the Security Officer.

(2) Notify the person responsible for the container and its contents.

(3) Lock the container.

b. When notified that a container of classified matter has been found unlocked and unattended, the individual responsible for the container shall check the contents for visible indications of tampering.

c. Persons who find classified matter out of safes and unattended shall immediately report such fact to the Head of the Department or to the Security Officer.

47. Record of locking and unlocking containers. - Officers responsible for TOP SECRET and SECRET matters shall maintain a record of the time and date the container is locked and unlocked.

48. Changing, recording and disseminating container combinations. -

a. Combinations shall be changed at least once every six (6) months and at such other times as deemed appropriate, and at the earliest practicable time following:

(1) The loss or possible compromise of the safe combination.

(2) The discharge, suspension or reassignment of any person having knowledge of the combination.

(3) The receipt of a container.

b. Identification numbers must be obliterated from combination padlocks prior to their use. Three-position dial-type combination padlocks, the combinations of which can be changed in the manner as those of locks built into safes, need not have the manufacturer's identification numbers obliterated.

49. Control of keys. - Keys shall be safeguarded as follows:

a. All keys shall be recorded in a control register and checked periodically.

b. All keys for containers of classified matter when not in use shall be placed in a locked box in the office under the care of a responsible officer.

c. Duplicate keys should be placed in a sealed container and kept in a combination safe.

d. The loss of a key must be reported to the Head of the Department or to the Security Officer.

e. Department Heads shall institute additional measures to safeguard keys appropriate to their respective offices.

Section XI

MISCELLANEOUS

50. Special procedures for safeguarding certain documents from foreign nationals. -

a. Classified information which should be withheld from foreign nationals shall be stamped or marked with a special handling notice as follows:

> SPECIAL HANDLING REQUIRED. RELEASE TO FOREIGN NATIONALS NOT AUTHORIZED EXCEPT _____ (enter "None" or names of representatives of foreign nations specifically authorized to have access to the document) BY AUTHORITY OF _____ (enter title or position of official authorized to determine which foreign nationals may have access to the document) DATE _____ (enter date).

51. Classified matter in the possession of individuals on travel orders. -

a. An individual on travel orders who is authorized to have in his possession classified matter shall safeguard such matter by one of the following methods:

(1) By contacting and availing of the storage facilities of the nearest respective field or branch office, or Armed Forces installation; or

(2) By keeping the matter under personal physical control at all times.

b. Personnel on travel status shall not carry classified matter across international borders where the classified matter may be liable to scrutiny by customs inspectors or other unauthorized individuals. Such matter should be sent in advance by diplomatic pouch or diplomatic courier only.

52. Emergency destruction. -

a. Plans. - Department Heads shall provide for emergency destruction or safe removal of all classified matter under their jurisdiction should civil disturbances, disaster or enemy action require such action.

b. Aboard airplane or ship. - If a craft carrying classified matter is forced down, stranded or shipwrecked on unfriendly territory or on neutral territory where capture appears imminent or, under any other circumstances where it appears unlikely that the classified matter can properly be protected, such matter shall be destroyed in any manner that will render recognition impossible, preferably by burning.

53. Security of typewriter ribbons. - Cotton, rayon, paper and silk typewriter ribbons are insecure until typed through at least twice. Insecure ribbons shall be appropriately safeguarded if used to type classified information. Nylon ribbons are secure at all times.

54. Classified waste. - Waste, such as preliminary drafts, notes, dictaphone- or other-type recordings, typewriter ribbons, carbon paper, stencils, stenographic notes, carbon plates, exposed film (developed or undeveloped) and similar items containing classified information shall be disposed of in a manner prescribed for similarly classified matter. Certificate of destruction is not required.

55. Supplementary security regulations. - Department Heads shall publish regulations to supplement this Executive Order to include measures appropriate to their respective Departments as indicated herein and to cover the following general subjects or circumstances:

a. Movement control of organic personnel and visitors within their respective jurisdictions.

b. Security arrangements in dealing with government contractors engaged in projects concerning classified matter.

c. Security measures to safeguard classified information transmitted through electronic communication facilities.

Department Heads shall seek the assistance of the Director, National Intelligence Coordinating Agency or of the Secretary of National Defense in preparing the above supplemental regulations.

56. Security Clearance. - The Head of the Department shall be responsible for the issuance of security clearances in his Department. In this regard he may coordinate directly with the National Intelligence Coordinating Agency or the Department of National Defense.

Section XII

ADMINISTRATIVE LIABILITY

57. Any violation of the provisions of these regulations shall be dealt with administratively by proper authorities. Said administrative proceeding shall be without prejudice to any criminal prosecution if the violation constitutes an offense under the provisions of the Revised Penal Code or any other penal law. The unauthorized publication of any classified information shall be deemed a violation of these regulations by the parties responsible therefor.

All executive orders, proclamations or circulars inconsistent herewith are hereby revoked.

By authority of the President:

CALIXTO O. ZALDIVAR
Acting Executive Secretary

Manila, August 14, 1964

ANNEX "A"

CERTIFICATE OF DESTRUCTION OF CLASSIFIED RECORDS — OFFICE

DATE OF DOCUMENT	CLASSIFICATION	RECEIPT IDENTIFICATION NO.	REFERENCE NO (SUBJECT)	ORIGINATING AGENCY	ADDRESS	AUTHORITY FOR DESTRUCTION

I CERTIFY THAT I HAVE THIS DATE RECEIVED FOR DESTRUCTION THE DOCUMENTS LISTED ABOVE.	DATE	SIGNATURE OF CUSTODIAN:
I CERTIFY THAT I HAVE THIS DATE DESTROYED IN ACCORDANCE WITH SECURITY REGULATIONS THE DOCUMENTS LISTED ABOVE.	DATE	SIGNATURE OF PERSON MAKING DESTRUCTION:
I CERTIFY THAT I HAVE THIS DATE WITNESSED THE DESTRUCTION OF THE ABOVE LISTED DOCUMENTS.	DATE	SIGNATURE OF WITNESSING OFFICER:

ANNEX "Ø"

OFFICIAL RECEIPT FOR CLASSIFIED MATTER

FROM : _____

_____

) : _____

_____

CONTROL NO. _____

FILE : _____

NO.: _____ of _____ Copies

I acknowledge to have received on this _____ day of _____ 196_____ at _____ Hr the following classified documents:

Brief Description	Classification

NOTE : _____

_____

_____

_____

_____

(SIGNATURE)

FULL NAME & DESIGNATION IN PRINT

OFFICE TEL. NO. _____

TOP SECRET

(Unclassified if not covering Top Secret Document)

THIS IS A COVER SHEET

WARNING:

THE UNAUTHORIZED DISCLOSURE OF THE INFORMATION CONTAINED IN ATTACHED DOCUMENT WOULD CAUSE EXCEPTIONALLY GRAVE DAMAGE OR DANGER TO THE NATION, EITHER POLITICALLY, ECONOMICALLY OR FROM A SECURITY OR MILITARY STANDPOINT.

RESPONSIBILITY OF PERSONS HANDLING ATTACHED DOCUMENT(S)

1. Do not leave the document(s) unattended except when properly secured.

2. Transfer the document(s) only to persons who need to know and who possess the required security clearance.

3. Obtain a receipt whenever relinquishing control of the document(s).

STORAGE:

Safe or its approved equivalent

REPRODUCTION:

The document may be copied, extracted or reproduced only when classifying authority has authorized such action. Reproduction should be under the supervision of an authorised officer/official.

DISPOSITION:

This cover sheet should be treated as part of the document to which it is attached and should be included when the document is permanently filed.

REQUIREMENT:

Anybody who handled, read or acted on attached document(s) shall sign in the appropriate space provided for in record of transmission on the other side of this cover sheet.

TOP SECRET

(Unclassified if not covering document)

RECORD OF TRANSMISSION OF CLASSIFIED DOCUMENT

Office of origin _____ DATE _____

SUBJECT OF CLASSIFIED DOCUMENT

Copy Nr_____ Nr of pages _____

PERSONNEL WHO HAVE HANDLED, READ AND/OR ACTED ON THE DOCUMENT

Signature over Printed name	Assignment	Date Rec'd	& Time Rel'd

(Unclassified if not covering document)

RECORD OF TRANSMISSION OF CLASSIFIED DOCUMENT

Office of origin _____ DATE _____

SUBJECT OF CLASSIFIED DOCUMENT

Copy Nr_____ Nr of pages _____

PERSONNEL WHO HAVE HANDLED, READ AND/OR ACTED ON THE DOCUMENT

Signature over Printed name	Assignment	Date Rec'd	& Time Rel'd

SECRET

(Unclassified if not covering Secret Document)

THIS IS A COVER SHEET

WARNING:

THE UNAUTHORIZED DISCLOSURE OF THE INFORMATION CONTAINED IN ATTACHED DOCUMENT(S) WOULD ENDANGER NATIONAL SECURITY, CAUSE SERIOUS INJURY TO THE INTEREST OR PRESTIGE OF THE NATION OR OF ANY GOVERNMENTAL ACTIVITY THEREOF OR WOULD BE OF GREAT ADVANTAGE TO A FOREIGN NATION.

RESPONSIBILITY OF PERSONS HANDLING THE ATTACHED DOCUMENT(S):

1. Do not leave the document(s) unattended except when properly secured.
2. Transfer the document(s) only to persons who need to know and who possess the required security clearance.
3. Obtain a receipt whenever relinquishing control of the document(s).

STORAGE:

Safe or its approved equivalent

REPRODUCTION:

Copies should not be made without consent of the originating agency.

DISPOSITION:

This cover sheet should be treated as part of the document to which it is attached and should be included when the document is permanently filed.

REQUIREMENT:

Anybody who handles [illegible] attached document(s) shall sign in the appropriate space provided for in record of transmission on the other side of this cover sheet.

SECRET

CONFIDENTIAL

(Unclassified if not covering Confidential document)

THIS IS A COVER SHEET

WARNING:

THE UNAUTHORIZED DISCLOSURE OF THE INFORMATION CONTAINED IN THE ATTACHED DOCUMENT(S) WHILE NOT ENDANGERING NATIONAL SECURITY WOULD BE PREJUDICIAL TO THE INTEREST OR PRESTIGE OF THE NATION, ANY GOVERNMENTAL ACTIVITY, OR WOULD CAUSE ADMINISTRATIVE EMBARRASSMENT OR UNWARRANTED INJURY TO AN INDIVIDUAL, OR WOULD BE OF ADVANTAGE TO A FOREIGN NATION.

RESPONSIBILITY OF PERSONS HANDLING THE ATTACHED DOCUMENT(S):

1. Do not leave the document(s) unattended except when properly secured.
2. Transfer the document(s) only to persons who need to know and who possess the required security clearance.
3. If so required obtain a receipt whenever relinquishing control of the document(s).

STORAGE:

Safe or filing cabinet with iron bar & combination padlock

REPRODUCTION:

Copies may be made of these documents except when the originating office has specifically stated that no copy shall be made without prior authority.

DISPOSITION:

This cover sheet need not be included when the original document is permanently filed.

CONFIDENTIAL

TABLE OF CONTENTS

		Paragraph	Page
SECTION I	GENERAL		
	Classification categories	1	1
	Definition of terms	2	1- 2
	Security Officers	3	2
SECTION II	TOP SECRET MATTER		
	Definition.	4	2- 3
	Classification Authority.	5	3
	Reproduction.	6	3
	Inventory	7	3
	Transmission.	8	3- 4
	Storage	9	4
	Destruction	10	4
SECTION III	SECRET MATTER		
	Definition.	11	4- 5
	Classification Authority.	12	5
	Reproduction.	13	5
	Transmission.	14	5
	Storage	15	5- 6
	Destruction	16	6
SECTION IV	CONFIDENTIAL MATTER		
	Definition.	17	6
	Classification Authority.	18	7
	Reproduction.	19	7
	Transmission.	20	7
	Storage	21	7
	Destruction	22	7
SECTION V	RESTRICTED MATTER		
	Definition.	23	7
	Authority to Classify, Reproduction, Dissemination and Destruction . .	24	7
SECTION VI	CLASSIFYING AND MARKING		
	General	25	7
	Rules for classification.	26	7- 8
	Classification marking.	27	8- 9
	Additional Markings	28	10
SECTION VII	CONTROL OF CLASSIFIED MATTER		
	Custody and accounting of classified matter.	29	10
	Unauthorized keeping of private records	30	10
	Dissemination	31	10
	Discussion involving classified matter	32	10-11
	Disclosure to other Departments of classified information originating from another Department	33	11
	Release of classified matter outside a Department.	34	11-12
	Removal of classified matter from offices for official use.	35	12
	Compromise or loss of classified matter.	36	12-13
SECTION VIII	REGRADING AND DECLASSIFICATION		
	Responsibility for regrading. . . .	37	13
	Downgrading or declassification . .	38	13

	Regrading	39	13
	Notification of change of classification	40	14
	Marking of regraded documents . . .	41	14
SECTION IX	TRANSMISSION OF CLASSIFIED MATTER		
	Classified document receipts . . .	42	14-15
	Cover Sheets	43	15
	Preparation of classified matter for transmission outside a Department	44	15-16
	Transmission within a Department .	45	16
SECTION X	SECURITY OF CONTAINERS		
	Unlocked containers	46	16
	Record of locking and unlocking containers	47	16
	Changing, recording and disseminating container combinations	48	16-17
	Control of keys	49	17
SECTION XI	MISCELLANEOUS		
	Special procedures for safeguarding certain documents from foreign nationals	50	17
	Classified matter in the possession of individuals on travel orders .	51	17-18
	Emergency destruction	52	18
	Security of typewriter ribbons . .	53	18
	Classified waste	54	18
	Supplementary security regulations.	55	18
	Security Clearance	56	18
SECTION XII	ADMINISTRATIVE LIABILITY	57	19

	Regrading	39	13
	Notification of change of classification	40	14
	Marking of regraded documents . . .	41	14
SECTION IX	TRANSMISSION OF CLASSIFIED MATTER		
	Classified document receipts . . .	42	14-15
	Cover Sheets	43	15
	Preparation of classified matter for transmission outside a Department	44	15-16
	Transmission within a Department .	45	16
SECTION X	SECURITY OF CONTAINERS		
	Unlocked containers	46	16
	Record of locking and unlocking containers	47	16
	Changing, recording and disseminating container combinations	48	16-17
	Control of keys	49	17
SECTION XI	MISCELLANEOUS		
	Special procedures for safeguarding certain documents from foreign nationals	50	17
	Classified matter in the possession of individuals on travel orders .	51	17-18
	Emergency destruction	52	18
	Security of typewriter ribbons . .	53	18
	Classified waste	54	18
	Supplementary security regulations.	55	18
	Security Clearance	56	18
SECTION XII	ADMINISTRATIVE LIABILITY	57	19

OFFICE OF THE PRESIDENT
OF THE PHILIPPINES

MEMORANDUM CIRCULAR NO. 196

AMENDING MEMORANDUM CIRCULAR 78 DATED AUGUST 14, 1964, ENTITLED "PROMULGATING RULES GOVERNING SECURITY OF CLASSIFIED MATTER IN GOVERNMENT OFFICES."

1. A new section, to be known as Section XII, is hereby inserted between Sections XI and XII of Memorandum Circular No. 78 dated August 14, 1964, providing security of classified matter in government offices, which reads as follows:

"SECTION XII

"COMMUNICATION SECURITY

"57. Communication Security

a. Definition – Communication Security is the protection resulting from the application of various measures which prevent or delay the enemy or unauthorized persons in gaining information through our communications. It includes Transmission, Cryptographic and Physical security.

b. Rules governing Communication Security do not in themselves guarantee security, and they do not attempt to meet every conceivable situation. Communication Security rules are a means, not an end in themselves.

c. Department Heads are responsible for the maintenance of communication security and for the promulgation of additional

directive a may be necessary to insure proper communication security control within their jurisdiction.

d. All communication personnel should have an appreciation of the basic principles of communication security since the neglect of a single aspect of communication security may result in compromise.

“58. Communication Security Officer:

a. A properly trained and cleared Communication Security Officer shall be appointed in every Department of the Government handling cryptographic communication.

“59 Responsibilities/Duties of the Communication Security Officer:

a. Responsible for the selection and training of cleared communication personnel to perform crypto duties.

b. Responsible for the operations and maintenance of the cryptocenter.

c. Conduct periodic inspection of the cryptocenter to ascertain that crypto materials are properly handled and accounted for and that all directives concerning crypto-operations are strictly observed.

d. Designate a custodian for crypto-matepials,

e. Publish an emergency destruction plan for classified materials.

f. Recommend measures to improve transmission, cryptographic and physical security.

g. Conduct investigation in case of less or compromise of crypto-materials in accordance with paragraph 36 above.

“60. Transmission Security:

a. Definition – Transmission Security is that component of communication security which results from all measures designed to protect transmission from interception, traffic analysis and imitative deception.

b. Communication personnel shall select the means most appropriate to accomplish the delivery of message in accordance with the specified precedence and security requirements.

c. All classified messages within the Government service which are transmitted electrically should be encoded, enciphered and/or encrypted.

d. All classified messages sent by commercial means shall be encoded, enciphered and/or encrypted.

e. No classified message shall be transmitted over a telephone system not equipped with security device.

f. The transmission by visual means of a classified message in plain language shall be authorized only after careful consideration has been given to the necessity for sending in plain language and to the possibility of interception by unauthorized persons.

g. Radio Operations shall adhere to the use of correct procedures, circuit discipline and authentication system as a security measures against traffic analysis, imitative deception and radio direction finding.

“61. Cryptographic Security:

a. Definition – Cryptographic Security is that component of communication security which results from the provisions of technically sound cryptosystem and their proper use.

b. Message should scrutinized prior to encryption giving particular attention to the security classification, precedence, and to any special handling or routing precautions that may be necessary.

c. Messages should be completely checked before transmission to insure that the operating instructions pertaining to the system used have been followed and that the encrypted text is decryptable.

“62. Physical Security:

a. Definition – Physical Security is that component of communication security which results from measures necessary to safeguard classified communication equipment and material from access thereto by unauthorized persons.

b. Physical security measures include handling of classifies materials, i.e., storage, accounting and destruction.”

2. Section XII of the same circular shall hereafter be known as Section XIII, and Item 57 as Item 63.

By authority of the President:
(SGD.) RAFAEL M. SALAS
Executive Secretary

Manila, July 19, 1968.

S. No. 2965
H. No. 4115

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

(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.

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, which 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).

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 be processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided, further,* That adequate safeguards are guaranteed by said laws authorizing their processing.

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.

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 be 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.

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 that 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.

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.

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.

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 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).

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 he 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 abovementioned 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 be applied.

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

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.

Approved,

FELICIANO BELMONTE JR.
Speaker of the House of Representatives

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.

MARILYN B. BARUA-YAP
Secretary General
House of Representatives

EMMA LIRIO-REYES
Secretary of the Senate

Approved: AUG 15 2012

BENIGNO S. AQUINO III
President of the Philippines

O

ANNEX E
DETAILED FOI REQUEST PROCESS

STEP I – PAO, AFP (FRO) Receives Request (1 Day)

- Receive Request
  - Stamp received
  - Provide copy to requestor
  - Log details on FOI tracker
- Initial evaluation
  - Completeness of request
  - Intent of request
  - Availability of the information

If ***denied***:
• Communicate denial to requesting party

If it ***passed the evaluation***:
• Forward to COU

STEP II – Chief, Admin Division (COU) Clarifies, Locates, & Reviews FOI; Request Security Clearance (10 Days)

- Cognizant Office/Unit (COU) receives endorsed request
- Forward to OJ2 for security clearance, if necessary
- Review request and prepare recommendations for the FDM on the approval or denial of the release of information to the requesting party

Information ***NOT found***:
• Communicate denial to requesting party through FRO

Information ***located***:
• Forward endorsed request, security clearance, and information requested to FDM

If an ***extension of time is required***:
• Communicate extension of time to the requesting party through the FRO

STEP III – CSAFP (FDM) Approves or Denies Release of Information Requested (3 Days)

- FDM shall refer to the guidelines set forth in the AFP FOI Manual and the recommendations provided by the COU in approving or denying the release of information requested

Information ***approved***:
• Communicate approval to the FRO for the release of information to the requesting party

Information ***denied***:
• Communicate denial through the FRO

STEP IV – PAO, AFP (FRO) Communicates Response (1 Day)

- FRO communicates response to the requesting party
- Update FOI tracker and save response

STEP V – Requesting Party Filed an Appeal with the TDCSAFP (CARC) (30 Days)

- The requesting party may file an appeal with the CARC within 15 days from notice of denial of the FOI Request
- Failure to appeal after the 15-day period shall be deemed a waiver of the right to appeal
- The CARC, through its FOI Appeals and Review Subcommittee (FARS), shall review, evaluate, and recommend approval or denial of the appeal to CSAFP within 30 days

Information ***approved***:
• Communicate approval to the FRO

Information ***denied***:
• Communicate denial through the FRO

ANNEX F

FOI REQUEST FORM

Name (Pangalan):
Address (Tirahan):
Contact No. (Mobile, Telephone, E-mail, & etc.):
Office/School Address (Lokasyon ng Opisina O Eskwelahan):
Age (Edad):
Gender (Kasarian):
Date of Request (Petsa ng Paghingi ng Impormasyon):
Please state the documents or information you are looking for. (Pakilahad po ang dokumento o impormasyon na inyong hinahanap.)
Please state the covered period of the said documents/information. (Pakilahad po ang panahong saklaw ng nasabing dokumento o impormasyon.)
Please adequately describe your purpose for securing these documents / information. (Pakilarawan po ng malinaw ang inyong layunin sa paghingi ng nasabing dokumento o impormasyon.)
Acknowledgment of Receipt of Document **(Pagkilala ng Pagtanggapng Dokumento)** **Name (Pangalan): _____** **Date & Time (Petsa at Oras): _____** **Lagda (Signature): _____**

Terms of Use: The requested information or document provided shall not be used: (a) for any purpose other than what is stated in the "FOI Request Form"; (b) for any purpose that is contrary to law, public policy, public order, morals, or good customs; and (c) reproduced for any commercial use. Any violation to the said Terms of Use may subject the requesting party to legal actions and/or penalties as may be provided by law.

Mga Tuntunin ng Paggamit: Anumang impormasyon o dokumentong ibinigay ay hindi maaring gagamitin: (a) para sa anumang layunin maliban sa kung ano ang nakasaad sa nilagdaang "FOI Request Form"; (b) para sa anumang layunin na salungat sa batas, pampublikong patakaran, pampublikong kaayusan, moralidad, o mabuting kaugalian; at (c) para sa anumang komersyal na paggamit. Anumang paglabag sa nasabing mga Tuntunin ng Paggamit ay may karampatang legal na aksyon at/o parusang naaayon sa batas.

ANNEX G

FOI APPEAL TEMPLATE

[Date]

Armed Forces of the Philippines

Dear Sir/Ma'am,

I submitted a request for information dated _____ asking for _____. Attached is a copy of the said request **(Tab A)**.

On _____, I received a notice **(Tab B)** denying the abovementioned request for the following reason: _____.

I would like to appeal this denial on the following ground/s: _____ _____ _____.

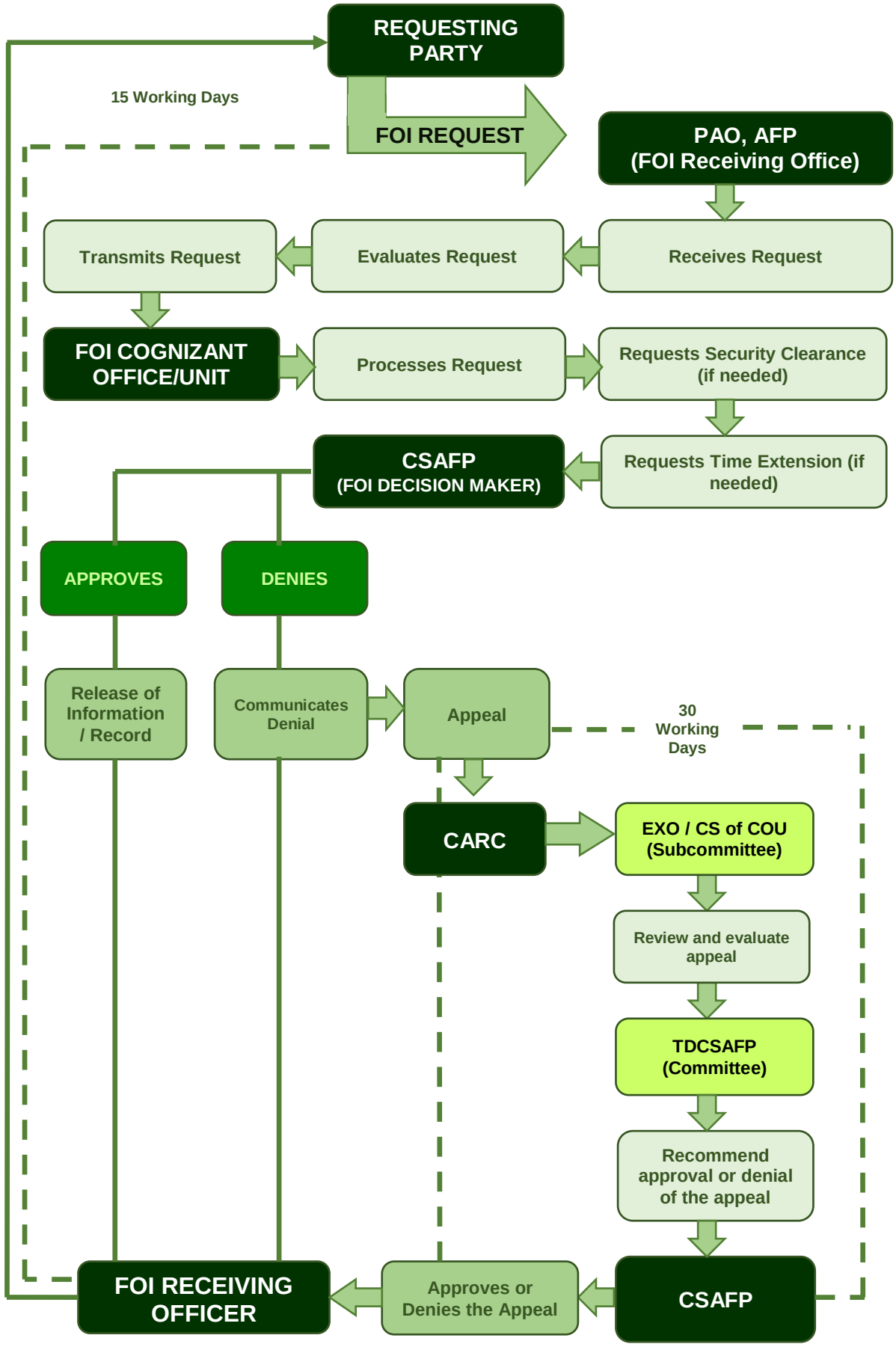
This appeal is being filed within fifteen (15) days from receipt of the notice of denial.

Thank you.

Respectfully,

Requesting Party

ANNEX H
FOI FLOW CHART



NOTE:
- - - number of working days

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 OF FULL PUBLIC DISCLOSURE AND TRANSPARENCY IN THE PUBLIC SERVICE AND PROVIDING GUIDELINES THEREFOR

WHEREAS, pursuant to Section 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 departments, 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 recordings, magnetic or other tapes, electronic data, computer-stored data, or 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, departments, bureaus, and instrumentalities, including government-owned or -controlled corporations, and state universities and colleges. Local government units (LGUs) are enjoined 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 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 laws or jurisprudence.

The Department 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 Department 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 as provided in Section 4 hereof.

The determination of the applicability of any of the exceptions to the request shall be the responsibility of the Head of the Office which has custody or control of the information, public record or official record, or of 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 an individual's right to privacy 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 laws, 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; and

(c) Any employee or official 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 regulations.

SECTION 8. People's Freedom of 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 information:

(a) The location and contact information of the head, regional, provincial, and field offices, and other established places where the public can submit requests to obtain information;
(b) The person or officer responsible for receiving requests for information;
(c) The procedure for the filing and processing of the request, as provided in the succeeding Section 9 of this Order;
(d) The standard forms for the submission of requests and for the proper acknowledgment of such requests;
(e) The process for the disposition of requests;
(f) The procedure for administrative appeal of any denial of request for access to information; and
(g) The schedule of applicable fees.

SECTION 9. Procedure. The following procedure shall govern the filing and processing of requests 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 of exceptions as hereinabove provided.

(b) The public official receiving the request shall provide reasonable assistance, free of charge, to enable all requesting parties, 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 or 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 the 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 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 events or other analogous cases. The government office shall

notify the person making the request of such extension, setting forth the reasons for the extension. In no case shall the extension go beyond twenty (20) working days counted from the end of the original period, 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 requested, 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 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 wholly or partially, it shall, as soon as practicable and within fifteen (15) working days from the receipt of the request, 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 for access to information.

SECTION 13. Remedies in Case of Denial of Request for Access to Information. A person whose request for access to information has been denied may avail himself of the remedies set forth below:

(a) Denial of any request for access to information may be appealed to the person or office next higher in authority, following the procedure mentioned in Section 8 (f) 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 shall 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 party may file the appropriate judicial action 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 and 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.

By the President:

SALVADOR C. MEDIALDEA
Executive Secretary

REPUBLIC OF THE PHILIPPINES
PRRD 2016 - 000156

CERTIFIED COPY:

MARIANITO M. DIMAANDAL
DIRECTOR IV
MALACAÑANG RECORDS OFFICE

7-25-2016

Office of the President
of the Philippines
Malacañang

MEMORANDUM FROM THE EXECUTIVE SECRETARY

TO: All Heads of Departments, Bureaus and Agencies of the National/Local Governments Including Government-Owned and Controlled Corporations (GOCCs), Government Financial Institutions (GFIs), and All Others Concerned

SUBJECT: **INVENTORY OF EXCEPTIONS TO EXECUTIVE ORDER NO. 2 (S. 2016)**

DATE: 24 November 2016

Pursuant to Section 4 of Executive Order (EO) No. 2 (s. 2016), the Office of the President hereby circularizes the inventory of exceptions to the right to access of information, for the guidance of all government offices and instrumentalities covered by EO No. 2 (s. 2016) and the general public.

The foregoing list of exceptions shall be without prejudice to existing laws, jurisprudence, rules or regulations authorizing the disclosure of the excepted information upon satisfaction of certain conditions in certain cases, such as the consent of the concerned party or as may be ordered by the courts.

In evaluating requests for information, all heads of offices are enjoined to ensure the meaningful exercise of the public of their right to access to information on public concerns.

For your information and guidance.

SALVADOR C. MEDIALDEA

CERTIFIED COPY:

MARIANITO M. DIMAANDAL
DIRECTOR IV
MALACAÑANG RECORDS OFFICE

Exceptions to Right of Access to Information

For the guidance of all government offices and instrumentalities covered by EO No. 2 (s. 2016) and the general public, the following are the exceptions to the right of access to information, as recognized by the Constitution, existing laws, or jurisprudence:[1]

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.

---

[1] 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.

For the implementation of the exceptions to the right of access to information, the following provide the salient details and legal bases that define the extent and application of the exceptions.

1. Information covered by Executive privilege:

   a. Presidential conversations, correspondences, and discussions in closed-door Cabinet meetings;[2] and

   b. Matters covered by deliberative process privilege, namely:

      i. advisory opinions, recommendations and deliberations comprising part of a process by which governmental decisions and policies are formulated; intra-agency or inter-agency recommendations or communications during the stage when common assertions are still in the process of being formulated or are in the exploratory stage; or information pertaining to the decision-making of executive officials;[3] and
      ii. information, record or document comprising drafts of decisions, orders, rulings, policy decisions, memoranda, etc.;[4]

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

   a. Information, record, or document that must be kept secret in the interest of national defense or security;[5]

   b. Diplomatic negotiations and other information required to be kept secret in the conduct of foreign affairs;[6] and

---

[2] This exception may only be invoked by the President and his close advisors. The extent of the privilege is defined by applicable jurisprudence: *Senate v. Ermita*, G.R. No. 169777, 20 April 2006, 488 SCRA 1; *Neri v. Senate Committee on Accountability of Public Officers and Investigations*, G.R. No. 180643, 4 September 2008, 564 SCRA 152; *Akbayan v. Aquino*, G.R. No. 170516, 16 July 2008, 558 SCRA 468; and *Chavez v. PCGG*, G.R. No. 130716, 9 December 1998, 299 SCRA 744.

[3] *Akbayan v. Aquino, supra*; *Chavez v. NHA*, G.R. No. 164527, 15 August 2007; and *Chavez v. PCGG, supra*. The privilege of invoking this exception ends when the executive agency adopts a definite proposition (*Department of Foreign Affairs v. BCA International Corp.*, G.R. No. 210858, 20 July 2016).

[4] Section 3(d) Rule IV, *Rules Implementing the Code of Conduct and Ethical Standards for Public Officials and Employees* (Rules on CCESPOE). Drafts of decisions, orders, rulings, policy decisions, memoranda, and the like, such as resolutions prepared by the investigating prosecutor prior to approval for promulgation and release to parties [*Revised Manual for Prosecutors of the Department of Justice (DOJ)*] are also covered under this category of exceptions.

[5] *Almonte v. Vasquez*, G.R. No. 95367, 23 May 1995, 244 SCRA 286; *Chavez v. PCGG, supra; Legaspi v. Civil Service Commission*, L-72119, 29 May 1987, 150 SCRA 530; *Chavez v. NHA, supra; Neri v. Senate, supra; Chavez v. Public Estates Authority*, G.R. No. 133250, 9 July 2002, 384 SCRA 152; and Section 3(a), Rule IV, Rules on CCESPOE. This exception generally includes matters classified under Memorandum Circular (MC) No. 78, as amended by MC No. 196 as "Top Secret," "Secret," "Confidential," and "Restricted."

[6] *Akbayan v. Aquino, supra;* Section 3(a) Rule IV, Rules on CCESPOE. This privilege may be invoked by the Department of Foreign Affairs and other government bodies involved in diplomatic negotiations.

c. Patent applications, the publication of which would prejudice national security and interests;[7]

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

a. Investigation records compiled for law enforcement purposes or information which if written would be contained in such records, but only to the extent that the production of such records or information would –

i. interfere with enforcement proceedings;
ii. deprive a person of a right to a fair trial or an impartial adjudication;
iii. disclose the identity of a confidential source and in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source; or
iv. unjustifiably disclose investigative techniques and procedures;[8]

b. Informer's privilege or the privilege of the Government not to disclose the identity of a person or persons who furnish information of violations of law to officers charged with the enforcement of law;[9]

c. When disclosure of information would put the life and safety of an individual in imminent danger;[10]

d. Any information given by informants leading to the recovery of carnapped vehicles and apprehension of the persons charged with carnapping;[11] and

e. All proceedings involving application for admission into the Witness Protection Program and the action taken thereon;[12]

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

---

[7] The applicability of this exception is determined by the Director General of the Intellectual Property Office and subject to the approval of the Secretary of the Department of Trade and Industry. Section 44.3 of the *Intellectual Property Code* (RA No. 8293, as amended by RA No. 10372).

[8] Section 3(f), Rule IV, Rules on CCESPOE; *Chavez v. PCGG*, *supra*. May be invoked by law enforcement agencies.

[9] *Akbayan v. Aquino*, *supra*; and Section 51, *Human Security Act of 2007* (RA No. 9372). May be invoked by law enforcement agencies.

[10] Section 3(b), Rule IV, Rules on CCESPOE.

[11] Section 19, *New Anti Carnapping Act of 2016* (RA No. 10883). May be invoked by law enforcement agencies.

[12] Section 7, *Witness Protection, Security and Benefit Act* (RA No. 6981).

a. Information of a personal nature where disclosure would constitute a clearly unwarranted invasion of personal privacy,[13] personal information or records,[14] including sensitive personal information, birth records,[15] school records,[16] or medical or health records;[17]

Sensitive personal information as defined under the *Data Privacy Act of 2012* refers to personal information:[18]

(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.

However, personal information may be disclosed to the extent that the requested information is shown to be a matter of public concern or interest, shall not meddle with or disturb the private life or family relations of the individual[19] and is not prohibited by any law or regulation. Any disclosure of personal information shall be in accordance with the principles of transparency, legitimate purpose and proportionality.[20]

Disclosure of personal information about any individual who is or was an officer or employee of a government institution shall be allowed, provided that such information relates to the position or functions of the individual, including: (1) the fact that the individual is or was an officer or employee of

---

[13] Section 3(e), Rule IV, Rules on CCESPOE.

[14] Sections 8 and 15, *Data Privacy Act of 2012* (RA No. 10173); *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 [Section 3(g), *Data Privacy Act of 2012*]; Article 26, Civil Code. May be invoked by National Privacy Commission and government personal information controllers.

[15] Article 7, *The Child and Youth Welfare Code* [Presidential Decree (PD) No. 603].

[16] Section 9(4), *Education Act of 1982* [Batas Pambansa (BP) Blg. 232].

[17] Medical and health records are considered as sensitive personal information pursuant to Section 3(l)(2), *Data Privacy Act of 2012*; See also Department of Health-Department of Science and Technology (DOST)-Philippine Health Insurance Corporation Joint Administrative Order No. 2016-0002 (Privacy Guidelines for the Implementation of the Philippine Health Information Exchange).

[18] Section 3(l), *Data Privacy Act of 2012*.

[19] Article 26(2), *Civil Code*.

[20] Section 11, *Data Privacy Act of 2012*.

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;[21]

b. Source of any news report or information appearing in newspapers, magazines or periodicals of general circulation obtained in confidence;[22] and

c. Records of proceedings and processes deemed confidential by law for the privacy and/or protection of certain individuals, such as children, victims of crime, witnesses to a crime or rehabilitated drug offenders, including those pertaining to the following:

(1) records of child and family cases;[23]
(2) children in conflict with the law from initial contact until final disposition of the case;[24]
(3) a child who is a victim of any offense under the *Anti-Child Pornography Act of 2009*, including the name and personal circumstances of the child, or the child's immediate family, or any other information tending to establish the child's identity;[25]
(4) a child witness, who is a victim of a crime, an accused of a crime, or a witness to a crime, including the name, address, telephone number, school, or other identifying information of a child or an immediate family of the child;[26]
(5) cases involving violence against women and their children, including the name, address, telephone number, school, business, address, employer, or other identifying information of a victim or an immediate family member;[27]
(6) trafficked persons, including their names and personal circumstances, or any other information tending to establish the identity of the trafficked person;[28]
(7) names of victims of child abuse, exploitation or discrimination;[29]

---

[21] Section 4, *Data Privacy Act of 2012*.

[22] *An Act to Exempt the Publisher, Editor or Reporter of any Publication from Revealing the Source of Published News or Information Obtained in Confidence* (RA No. 53), as amended by RA No. 1477. May be invoked by government newspapers.

[23] Section 12, *Family Courts Act of 1997* (RA Act No. 8369).

[24] Section 43, *Juvenile Justice and Welfare Act of 2006* (RA No. 9344).

[25] Section 13, *Anti-Child Pornography Act of 2009* (RA No. 9775).

[26] Section 31, A.M. No. 00-4-07-SC, *Re: Proposed Rule on Examination of a Child Witness*.

[27] Section 44, *Anti-Violence Against Women and their Children Act of 2004* (RA No. 9262); and *People v. Cabalquinto*, G.R. No. 167693, 19 September 2006.

[28] Section 7, *Anti-Trafficking in Persons Act of 2003* (RA No. 9208), as amended by RA No. 10364.

[29] Section 29, *Special Protection of Children Against Abuse, Exploitation and Discrimination Act* (RA No. 7610).

(8) disclosure which would result in undue and sensationalized publicity of any case involving a child in conflict with the law, child abuse, or violation of anti-trafficking of persons;[30]

(9) records, documents and communications of proceedings involving domestic and inter-country adoptions, including the identity of the child, natural parents and adoptive parents;[31]

(10) names of students who committed acts of bullying or retaliation;[32]

(11) first time minor (drug) offenders under suspended sentence who comply with applicable rules and regulations of the Dangerous Drugs Board and who are subsequently discharged; judicial and medical records of drug dependents under the voluntary submission program; and records of a drug dependent who was rehabilitated and discharged from treatment and rehabilitation centers under the compulsory submission program, or who was charged for violation of Section 15 (use of dangerous drugs) of the *Comprehensive Dangerous Drugs Act of 2002*, as amended; and [33]

(12) identity, status and medical records of individuals with Human Immunodeficiency Virus (HIV), as well as results of HIV/Acquired Immune Deficiency Syndrome (AIDS) testing;[34]

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, such as but not limited to the following:

a. Trade secrets, intellectual property, business, commercial, financial and other proprietary information;[35]

---

[30] Section 14, *Juvenile Justice and Welfare Act of 2006*; Section 7, *Anti-Trafficking in Persons Act of 2003*, as amended; and Section 29, *Special Protection of Children Against Abuse, Exploitation and Discrimination Act*.

[31] Section 15, *Domestic Adoption Act of 1998* (RA No. 8552) and Section 43, IRR of RA No. 8552; Sections 6 and 16(b), *Inter-Country Adoption Act of 1995* (RA No. 8043) and Sections 53, 54 and 55 of IRR of RA No. 8043.

[32] Section 3(h), *Anti-Bullying Act* (RA No. 10627).

[33] Sections 60, 64 and 67, *Comprehensive Dangerous Drugs Act of 2002* (RA No. 9165).

[34] Sections 2(b), 18, 30, and 32, *Philippine AIDS Prevention and Control Act of 1998* (RA No. 8504).

[35] Sections 45, 106.1, and 150.2, *The Intellectual Property Code* (RA No. 8293, as amended by RA No. 10372); Section 66.2, *Securities Regulation Code* (RA No. 8799); DOST Administrative Order No. 004-16; Section 142, *The Corporation Code* (BP Blg. 68); Section 34, *Philippine Competition Act* (RA No. 10667); Sections 23 and 27 (c), *The New Central Bank Act* (RA No. 7653); *Anti-Money Laundering Act* (RA No. 9160); Section 18, *Strategic Trade Management Act* (RA No. 10697); Sections 10 and 14, *Safeguard Measures Act* (RA No. 8800); Section 12, *Toxic Substances and Hazardous and Nuclear Wastes Control Act of 1990* (RA No. 6969); Article 290, *Revised Penal Code*; Section 10.10, Rule 10, 2012 Revised IRR of *Build-Operate-Transfer Law* (RA No. 6957); and *Revised Philippine Ports Authority Manual of Corporate Governance*.

b. Data furnished to statistical inquiries, surveys and censuses of the Philippine Statistics Authority (PSA);[36]

c. Records and reports submitted to the Social Security System by the employer or member;[37]

d. Information gathered from HIV/AIDS contact tracing and all other related health intelligence activities;[38]

e. Confidential information submitted to the Philippine Competition Commission prohibited from disclosure by law, including the identity of the person who provided the information under condition of anonymity;[39]

f. Applications and supporting documents filed pursuant to the *Omnibus Investments Code of 1987*;[40]

g. Documents submitted through the Government Electronic Procurement System;[41]

h. Information obtained from accessing any electronic key, electronic data message, or electronic document, book, register, correspondence, information or other material pursuant to any powers conferred under the *Electronic Commerce Act of 2000*;[42]

i. Any confidential information supplied by the contractors in mineral agreements, and financial or technical assistance agreements pursuant to the *Philippine Mining Act of 1995* and its Implementing Rules and Regulations (IRR), during the term of the project to which it relates;[43]

j. Information received by the Department of Tourism (DOT) in relation to the accreditation of accommodation establishments (such as hotels and resorts) and travel and tour agencies;[44]

---

[36] Section 26, *Philippine Statistical Act of 2013* (RA No. 10625); and Section 4, *Commonwealth Act No. 591*. May be invoked only by the PSA.

[37] Section 24(c), *Social Security Act of 1997* (RA No. 1161, as amended by RA No. 8282).

[38] Section 29, *Philippine AIDS Prevention and Control Act of 1998* (RA No. 8504).

[39] Section 34, *Philippine Competition Act* (PCA), RA No. 10667 and Section 13, Rule 4 of the IRR of PCA. This exception can be invoked by the Philippine Competition Commission subject to well-defined limitations under the PCA.

[40] Section 81, EO No. 226 (s. 1987), as amended.

[41] Section 9, *Government Procurement Reform Act* (RA No. 9184).

[42] Section 32, *Electronic Commerce Act of 2000* (RA No. 8792).

[43] Section 94(f), *Philippine Mining Act of 1995* (RA No. 7942).

[44] Section 1, Rule IX, DOT MC No. 2010-02 (Rules and Regulations to Govern, the Accreditation of Accommodation Establishments – Hotels, Resorts and Apartment Hotels); and Section 23, DOT MC No. 2015-06 (Revised Rules and Regulations to Govern the Accreditation of Travel and Tour Agencies).

k. The fact that a covered transaction report to the Anti-Money Laundering Council (AMLC) has been made, the contents thereof, or any information in relation thereto;[45]

l. Information submitted to the Tariff Commission which is by nature confidential or submitted on a confidential basis;[46]

m. Certain information and reports submitted to the Insurance Commissioner pursuant to the *Insurance Code*;[47]

n. Information on registered cultural properties owned by private individuals;[48]

o. Data submitted by a higher education institution to the Commission on Higher Education (CHED);[49] and

p. Any secret, valuable or proprietary information of a confidential character known to a public officer, or secrets of private individuals;[50]

6. Information of which a premature disclosure would:

a. in the case of a department, office or agency which agency regulates currencies, securities, commodities, or financial institutions, be likely to lead to significant financial speculation in currencies, securities, or commodities, or significantly endanger the stability of any financial institution; or

b. be likely or significantly frustrate implementation of a proposed official action, except such department, office or agency has already disclosed to the public the content or nature of its proposed action, or where the department, office or agency is required by law to make such disclosure on its own initiative prior to taking final official action on such proposal.[51]

7. Records of proceedings or information from proceedings which, pursuant to law or relevant rules and regulations, are treated as confidential or privileged, including but not limited to the following:

---

[45] Section 9(c), *Anti-Money Laundering Act of 2001*, as amended. May be invoked by AMLC, government banks and its officers and employees.

[46] Section 10, *Safeguard Measures Act.*

[47] Section 297 in relation with Section 295 and Section 356, *The Insurance Code* (as amended by RA No. 10607).

[48] Section 14, *National Cultural Heritage Act of 2009* (RA No. 10066).

[49] CHED Memorandum Order No. 015-13, 28 May 2013.

[50] Articles 229 and 230, *Revised Penal Code*; Section 3(k), *Anti-Graft and Corrupt Practices Act* (RA No. 3019); Section 7(c), *Code of Conduct and Ethical Standards for Public Officials and Employees* (RA No. 6713); Section 7, *Exchange of Information on Tax Matters Act of 2009* (RA No. 10021); and Section 6.2, *Securities Regulation Code* (RA No. 8799).

[51] Section 3(g), Rule IV, Rules on CCESPOE.

a. Mediation and domestic or international arbitration proceedings, including records, evidence and the arbitral awards, pursuant to the *Alternative Dispute Resolution Act of 2004*;[52]

b. Matters involved in an Investor-State mediation;[53]

c. Information and statements made at conciliation proceedings under the *Labor Code*;[54]

d. Arbitration proceedings before the Construction Industry Arbitration Commission (CIAC);[55]

e. Results of examinations made by the Securities and Exchange Commission (SEC) on the operations, books and records of any corporation, and all interrogatories propounded by it and the answers thereto;[56]

f. Information related to investigations which are deemed confidential under the *Securities Regulations Code*;[57]

g. All proceedings prior to the issuance of a cease and desist order against pre-need companies by the Insurance Commission; [58]

h. Information related to the assignment of the cases to the reviewing prosecutors or the undersecretaries in cases involving violations of the *Comprehensive Dangerous Drugs Act of 2002*;[59]

i. Investigation report and the supervision history of a probationer;[60]

j. Those matters classified as confidential under the *Human Security Act of 2007*;[61]

---

[52] Sections 9, 23 and 33, *Alternative Dispute Resolution (ADR) Act of 2004* (RA No. 9285); and DOJ Circular No. 98 (s. 2009) or the IRR of the ADR Act.

[53] Article 10, International Bar Association Rules for Investor-State Mediation.

[54] Article 237, *Labor Code*.

[55] Section 7.1, Rule 7, CIAC Revised Rules of Procedure Governing Construction Arbitration.

[56] Section 142, *Corporation Code*. May be invoked by the SEC and any other official authorized by law to make such examination.

[57] Sections 13.4, 15.4, 29.2 (b), and 64.2 of the *Securities Regulation Code*.

[58] Section 53(b)(1) of the *Pre-Need Code of the Philippines*. The confidentiality of the proceedings is lifted after the issuance of the cease and desist order.

[59] DOJ Department Circular No. 006-16 (No. 6), 10 February 2016.

[60] Section 17, *Probation Law of 1976* [PD No. 968 (s.1976)].

[61] Sections 9, 13, 14, 29, 33 and 34, *Human Security Act of 2007* (RA No. 9372).

k. Preliminary investigation proceedings before the committee on decorum and investigation of government agencies;[62] and

l. Those information deemed confidential or privileged pursuant to pertinent rules and regulations issued by the Supreme Court, such as information on disbarment proceedings, DNA profiles and results, or those ordered by courts to be kept confidential;[63]

8. Matters considered confidential under banking and finance laws and their amendatory laws, such as:

a. RA No. 1405 (*Law on Secrecy of Bank Deposits*);

b. RA No. 6426 (*Foreign Currency Deposit Act of the Philippines*) and relevant regulations;

c. RA No. 8791 (*The General Banking Law of 2000*);

d. RA No. 9160 (*Anti-Money Laundering Act of 2001*); and

e. RA No. 9510 (*Credit Information System Act*);

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

a. Those deemed confidential pursuant to treaties, executive agreements, other international agreements, or international proceedings, such as:

(1) When the disclosure would prejudice legitimate commercial interest or competitive position of investor-states pursuant to investment agreements;[64]
(2) Those deemed confidential or protected information pursuant to United Nations Commission on International Trade Law Rules on Transparency in Treaty-based Investor-State Arbitration and Arbitration Rules (UNCITRAL Transparency Rules);[65] and
(3) Refugee proceedings and documents under the *1951 Convention Relating to the Status of Refugees*, as implemented by DOJ Circular No. 58 (s. 2012);

---

[62] Section 14, Civil Service Commission Resolution No. 01-0940.

[63] Section 18, Rule 139-B and Section 24, Rule 130 of the Rules of Court; and Section 11 of the Rule on DNA Evidence, A.M. No. 06-11-5-SC.

[64] Examples: Article 20 (2), ASEAN Comprehensive Investment Agreement; Article 15 (2) Agreement on Investment under the Framework Agreement on the Comprehensive Economic Cooperation between the ASEAN and the Republic of India; and Article 15 (2) of the Agreement on Investment under the Framework Agreement on the Comprehensive Economic Cooperation among the Government of the Member Countries of the ASEAN and the Republic of Korea.

[65] Article 7, UNCITRAL Transparency Rules.

b. Testimony from a government official, unless pursuant to a court or legal order;[66]

c. When the purpose for the request of Statement of Assets, Liabilities and Net Worth is any of the following:

   (1) any purpose contrary to morals or public policy; or
   (2) any commercial purpose other than by news and communications media for dissemination to the general public;[67]

d. Lists, abstracts, summaries of information requested when such lists, abstracts or summaries are not part of the duties of the government office requested;[68]

e. Those information and proceedings deemed confidential under rules and regulations issued by relevant government agencies or as decided by the courts;[69]

f. Requested information pertains to comments and disclosures on pending cases in judicial proceedings;[70] and

g. Attorney-client privilege existing between government lawyers and their client.[71]

---

[66] *Senate v. Neri*, *supra*; *Senate v. Ermita*, *supra*.

[67] Section 8(D), *Code of Conduct and Ethical Standards for Public Officials and Employees*.

[68] *Belgica v. Ochoa*, G.R. No. 208566, 19 November 2013; and *Valmonte v. Belmonte Jr.*, G.R. No. 74930, 13 February 1989, 252 Phil. 264.

[69] Examples: 2012 Guidelines and Procedures in the Investigation and Monitoring of Human Rights Violations and Abuses and the Provision of CHR Assistance; Government Service Insurance System's Rules of Procedure of the Committee on Claims; National Labor Relations Commission Resolution No. 01-02, Amending Certain Provisions of the New Rules of Procedure of the National Labor Relations Commission, 08 March 2002; Department of Agrarian Reform MC No. 07-11, 19 July 2011; Department of Social Welfare and Development MC No. 021-12, 16 October 2012; and Section 42, *Investment Company Act* (RA No. 2629); When the information requested is not a matter of public concern or interest as decided in *Hilado v. Judge Amor A. Reyes*, G.R. No. 163155, 21 July 2006.

[70] *Romero v. Guerzon*, G.R. No. 211816, 18 March 2015.

[71] Canon 21 of the *Code of Professional Responsibility*.

OFFICE OF THE PRESIDENT
OF THE PHILIPPINES

MEMORANDUM CIRCULAR NO. 78

PROMULGATING RULES GOVERNING SECURITY OF CLASSIFIED MATTER IN GOVERNMENT OFFICES.

The following regulations entitled "SECURITY OF CLASSIFIED MATTER IN GOVERNMENT DEPARTMENTS AND INSTRUMENTALITIES" for safeguarding official matters affecting the national security, to be enforced and observed in all departments, bureaus, offices and agencies of the government in all national, provincial, municipal and city levels, are hereby promulgated:

SECURITY OF CLASSIFIED MATTER IN
GOVERNMENT DEPARTMENTS & INSTRUMENTALITIES

Section I

GENERAL

1. Classification categories. -

a. Official matter which requires protection in the interest of national security shall be limited to four categories of classification which, in descending order of importance, shall carry one of the following designations:

(1) TOP SECRET
(2) SECRET
(3) CONFIDENTIAL
(4) RESTRICTED

b. The classifications mentioned in sub-paragraph a above shall not be attached to a matter which does not involve the national security or which does not relate to any one of those specifically enumerated in paragraphs 4, 11, 17, and 23, below.

2. Definition of terms. -

a. The term "Department" is used to cover any Philippine Government Department, Service, or Instrumentality.

b. The term "matter" includes everything, regardless of its physical character, on or in which information is recorded or embodied. Documents, equipment, projects, books, reports, articles, notes, letters, drawings, sketches, plans, photographs, recordings, machinery, models, apparatus, devices, and all other products or substances fall within the general term "matter". Information which is transmitted orally is considered as "matter" for purposes of security.

c. The term "officer" includes any Government or Armed Forces official of officer permanently or temporarily employed in a Department as defined in a.

d. The term "document" covers any form of recorded information, including printed, written, drawn or painted matter, sound recordings, photographs, films, etc. "Documents" are included in "matter"

e. The term "equipment" includes machinery, apparatus, devices, supplies, ammunition, etc.

f. "Security Clearance" is the certification by a responsible authority that the person described is cleared for access to classified matter at the appropriate level.

write 2

g. The term "need to know" is the principle whereby access to classified matter may only be given to those persons to whom it necessary for the fulfillment of their duties. Persons are not e to have access to classified matter solely by virtue of their stat

h. The term "custodian" is an individual who has possession of or is otherwise charged with the responsibility for safeguarding and accounting of classified material.

i. "Certificate of Destruction" is the certification by a witnessing officer that the classified matter described therein has been disposed of, in his presence, by approved destruction methods (ANNEX A).

j. The term "physical security" is the safeguarding by physical means, such as guards, fire protection measures and other similar means, of information, personnel, property, utilities, facilities and installations against compromise, trespass, sabotage, pilferage, theft, espionage or any other dishonest or criminal act.

3. Security Officers. - A properly trained and cleared Security Officer shall be appointed in every Department of the Government which handles classified matter. He shall undergo training to be conducted by the National Intelligence Coordinating Agency or Armed Forces of the Philippines intelligence agencies. He shall be responsible to the Head of the Department for the implementation and enforcement of these regulations and the necessary action on breaches of security. Before appointment as a Security Officer, an officer must first be cleared by the Head of the Department for access to the highest classified matter the Department is authorized to handle. In providing this clearance, the Head of the Department may coordinate with the National Intelligence Coordinating Agency or the Department of National Defense.

Section II

TOP SECRET MATTER

4. Definition. - Information and material (matter) the unauthorized disclosure of which would cause exceptionally grave damage to the nation, politically, economically, or from a security aspect. This category is reserved for the nation's closest secrets and is to be used with great reserve.

Examples:

a. Very important political documents dealing with such matters as negotiations for major alliances.

b. Major governmental projects such as drastic proposals to adjust the nation's economy (before official publication).

c. Matter relating to new and far reaching experimental, technical and scientific developments in methods of warfare or defense, e.g., vital matter relating to atomic warfare, defense against biological warfare, or matter affecting future operational strategy. A TOP SECRET grading is justified if:

(1) It is likely to influence military strategy materially;

(2) It gives us a prolonged military advantage over other nations;

(3) It is liable to compromise some other project similarly graded.

d. Critical information relating to vital strategic areas and the supply of vital strategic materials.

e. Information which would indicate the capabilities or major successes of our intelligence services or which would imperil secret sources.

f. Critical information about cryptography in so far as it relates to devices and equipment under development.

g. Certain compilations of data or items which individually may be classified SECRET or lower, but which collectively should be put in a higher grade.

5. Classification Authority. -

a. Original classification authority for assignment of TOP SECRET classification rests exclusively with the Head of the Department. This power may, however, be delegated to authorized officers in instances when the necessity for such arises.

b. Derivative classification authority for TOP SECRET classification may be granted those officers who are required to give comments or responses to a communication that necessitates TOP SECRET response.

6. Reproduction. -

a. TOP SECRET matter may be copied, extracted, or reproduced only when the classifying authority has authorized such action. Permission to reproduce shall not extend beyond a specified number of copies which are to be accorded the same treatment as the original. At the time of issuance of any TOP SECRET document, the classifying authority shall insure that each copy of the document contains a notation substantially as follows:

(1) "Reproduction of this document in whole or in part is prohibited except with the permission of the issuing office or higher authority;" or

(2) "Reproduction of paragraph(s) _____ of this document is prohibited except with the permission of the issuing office or higher authority; other paragraphs may be reproduced."

b. The reproduction of TOP SECRET matter shall be carried out under the supervision of an authorized officer. All materials and waste incidental to the reproduction shall be accounted for and disposed of as prescribed in sub-paragraph 10a below.

7. Inventory. - The Head of the Department shall require physical inventory of all TOP SECRET matter in the custody of his Department at least once a year. Appropriate action on custodial deficiencies shall be made.

8. Transmission. -

a. TOP SECRET matter in the clear shall be transmitted

by any of the following means:

(1) By direct contact of officers concerned.

(2) By the officially designated courier.

(3) By accompanied Department of Foreign Affairs diplomatic pouch.

b. TOP SECRET matter shall not be transmitted by mail, express or electrical means, unless in cryptographic form.

9. Storage. - TOP SECRET matter shall be stored -

a. In a safe, steel file cabinet or other steel container equipped with a built-in, three-position, dial-type combination lock which is of such weight, size and construction as to minimize possibility of physical theft or damage by fire or tampering.

b. In a secure room or vault which is approved for such use by the Head concerned and which assures protection comparable to sub-paragraph a above.

10. Destruction. - TOP SECRET matter, which becomes eligible for destruction in accordance with approved schedules, shall be destroyed as prescribed below:

a. Destruction shall be accomplished by burning or pulping by the custodian in the presence of a witnessing officer designated by the responsible Head. Witnessing personnel must have a TOP SECRET clearance.

b. A certificate of destruction shall be prepared and forwarded to the originating office.

Section III

SECRET MATTER

11. Definition. - Information and material (matter) the unauthorized disclosure of which would endanger national security, cause serious injury to the interest or prestige of the nation or of any governmental activity or would be of great advantage to a foreign nation.

Examples:

a. High level directives dealing with important negotiations (as distinct from major negotiations which would be in the TOP SECRET category) with other countries.

b. Proposals for new schemes of governmental or other controls, foreknowledge of which would seriously prejudice their operation.

c. Matter relating to certain new methods of warfare or defence, including scientific and technical developments, not classified as TOP SECRET, e.g., new designs of Service aircraft, guided projectiles, tanks, radar and anti-submarine devices. A SECRET grading is justified if:

(1) It materially influences a major aspect of military tactics;

(2) It involves a novel principle applicable to existing important projects;

(3) It is sufficiently revolutionary to result in a major advance in existing techniques or in the performance of existing secret weapons;

(4) It is liable to compromise some other projects already so graded.

d. Plans or details of schemes for the defense of areas other than vital strategic areas, including plans or particulars of operations connected with them.

e. Vital military information, including photographs, maps, etc., relating to important defenses, establishments, and installations.

f. Intelligence which is not in the TOP SECRET category but which would reveal a secret source, or the value of which depends upon concealing the fact that we possess it.

g. Cryptographic devices and equipment unless specifically assigned to a lower classification.

h. Certain compilations of data or items which individually may be classified CONFIDENTIAL or lower, but which collectively should be put in a higher grade.

12. Classification Authority. - Same as for TOP SECRET matter.

13. Reproduction. - Same as for TOP SECRET matter.

14. Transmission - SECRET matter shall be transmitted as indicated below:

a. Between points within the Philippines:

(1. Direct contact of officers concerned.

(2) Electrical means in cryptographic form.

(3) Courier specifically authorized by the transmitting agency.

(4) Philippine registered mail.

b. Between points from within and outside the Philippines and vice-versa, and between points outside the Philippines:

(1) As authorized in sub-paragraphs 14a(1) through (3) above.

(2) Accompanied Department of Foreign Affairs diplomatic pouch.

15. Storage. - SECRET matter shall be stored in a manner authorized for TOP SECRET documents, or in metal file cabinets equipped with a steel lockbar and combination padlock of which the manufacturer's identification numbers have been obliterated. The file cabinets must be of such size, weight, construction or installation so as to minimize the chance of unauthorized physical removal or the possibility of persons gaining

unauthorized access by transferring or manipulation or damage by fire.

16. Destruction. - Same as for TOP SECRET matter except that the witnessing officer need have SECRET clearance only and that no certificate of destruction need be prepared. Only records of destruction shall be maintained.

Section IV

CONFIDENTIAL MATTER

17. Definition. - Information and material (matter) the unauthorized disclosure of which, while not endangering the National Security, would be prejudicial to the interest or prestige of the nation or any government activity, or would cause administrative embarrassment or unwarranted injury to an individual or would be of advantage to a foreign nation.

Examples:

a. Plans of Government projects such as land development, hydro-electric schemes, road development, or development of areas.

b. Routine Service reports, e.g., on operations and exercises, which contain information of value but not of vital interest to a foreign power.

c. Routine Intelligence reports.

d. Technical matter not of major importance but which has a distinct military value or requires protection otherwise, e.g., new weapons calculated to influence minor tactics or Service tests of war equipment of a standard pattern. A CONFIDENTIAL grading is justified if:

(1) It is more than a routine modification or logical improvement of existing materials and is sufficiently advanced to result in substantial improvement in the performance of existing CONFIDENTIAL weapons;

(2) It is sufficiently important potentially to make it desirable to postpone knowledge of its value reaching a foreign nation;

(3) It is liable to compromise some other project already so graded.

e. Certain personnel records and staff matters.

f. Certain compilations of data or items which individually may be classified RESTRICTED, or which may be unclassified, but the aggregation of which enhances their security value.

g. Matters, investigations and documents of a personal and disciplinary nature, the knowledge of which is desirable to safeguard for administrative reasons.

h. Identification of personnel being investigated for misconduct, anomaly or fraud prior to the filing of appropriate charges or completion of the findings of boards created for such purpose.

18. Classification Authority. - Any officer is authorized to assign CONFIDENTIAL classification to any matter in the performance of his duties.

19. Reproduction. - The copying, extracting from or reproduction of CONFIDENTIAL matter is authorized except when the originator or higher authority has specifically denied this authority.

20. Transmission. - Same as for SECRET matter.

21. Storage. - Same as for SECRET matter.

22. Destruction. - Same as for SECRET matter except that the presence of a witnessing officer and records of destruction are not required.

Section V

RESTRICTED MATTER

23. Definition. - Information and material (matter) which requires special protection other than that determined to be TOP SECRET, SECRET or CONFIDENTIAL.

Examples:

a. Departmental books of instruction and training and technical documents intended for official use only or not intended for release to the public.

b. Routine information relating to the supply and procurement of military stores.

c. Minor modifications and routine tests of equipment.

d. Certain compilations of data or items which individually may be reclassified but which in the aggregate warrant a classification.

24. Authority to Classify, Reproduction, Dissemination, and Destruction. - Authority to classify shall be the same as for CONFIDENTIAL matter. Reproduction is authorized. Transmission shall be through the normal dissemination system. Destruction shall be the same as for that of CONFIDENTIAL matter.

Section VI

CLASSIFYING AND MARKING

25. General. - The originators of classified matter shall be responsible for its proper classification. Overclassification should be avoided because it prejudices the integrity of the classification system, depreciates the importance of correctly classified matter and creates unnecessary delay, expense and administrative burden.

26. Rules for classification. -

a. Documents shall be classified according to their content.

b. The overall classification of a file or a group of physically connected documents shall be at least as high as that of the highest classified document therein. Pages, paragraphs, sections or components thereof may bear different classifications. Documents separated from the file or group shall be handled in accordance with their individual classifications.

c. Transmittal documents or indorsements which do not contain classified information or which contain information classified lower than that of the preceding element or inclosure shall include a notation for automatic downgrading.

d. Correspondence, indices, receipts, reports of possession, transfer or destruction, catalogs or accession lists shall not be classified if any reference to classified matter does not disclose classified information.

e. Classified matter obtained from other Departments shall retain the same original classification.

f. Classified matter furnished to the Philippine Government by a foreign government or international organization shall be assigned a classification which will assure a degree of protection equivalent to that required by the government or international organization which furnished the classified matter. In addition, any special handling instruction shall be complied with.

27. Classification marking. - Classified matter shall be marked as follows:

a. Unbound documents. - The assigned classification for unbound documents, such as letters, memoranda, reports, telegrams and similar documents, the pages of which are not permanently and securely fastened together, shall be marked or stamped (not typed) conspicuously at the top and bottom of all pages which contain classified information. In marking, stamping, or printing the classification categories, the letters shall be larger than the normal lettering of the rest of the document. Front and back covers, and title pages, when used; first pages; and any routing instructions or other papers of any size which conceal or partially conceal the cover, the title or first page shall bear the marking of the overall classification of the document. Other pages, except pages of messages to be transmitted electrically, shall be marked according to the classification of their own content. A cover shall be marked on its outer surface.

b. Permanently bound documents. - A permanently bound document is defined as one from which the pages cannot be removed without damage or mutilation. The classification of permanently bound documents, such as books or pamphlets shall be conspicuously marked, stamped or printed in letters larger than the normal lettering of the rest of the cover or page, at the top and bottom, on the first and back pages, and on the outside of the back cover.

c. Paragraphs, chapters, or sections. - The classification of a paragraph, chapter or section shall be indicated by including the initial of the appropriate classification in parenthesis at the end of such paragraph, chapter or section. Unclassified parts of classified documents will be marked "(U)".

d. Reproduction. - All copies or reproduction of classified matter shall be marked in the same manner as the original.

e. Photographs, films, and recordings. -

(1) Photographs - Negatives shall be marked with the appropriate classification markings and kept in containers bearing conspicuous classification markings. Roll negatives shall be marked at the beginning and end of each strip. Single negatives shall be marked with the appropriate classification. The top and bottom of each photographic print and the center of the reverse side shall be marked with the appropriate classification.

(2) Motion picture films - Classified motion picture films shall be marked at the beginning and end of each roll and in the title of each film, and shall be kept in containers bearing conspicuous classification markings.

(3) Sound recordings - Classified sound recordings shall be marked on readily observable portions with the appropriate markings, preferably at the beginning and at the end; when stored, the container shall display similar markings. When possible the classification shall be announced at the beginning and end of recordings.

f. Charts, maps, and drawings.- Classified charts, maps and drawings shall carry the classification marking under the legend, title block, or scale in such a manner that it can be reproduced on all copies made therefrom. Such classification shall also be prominently marked at the top and bottom in each instance and, if the document is rolled or folded, on the back in a clearly visible place.

g. Products or substances. - The assigned classification shall be conspicuously marked on classified products or substances and on their containers, if possible. If the article or container cannot be marked or if it is necessary to conceal the classified nature of the material, written notification of the classification shall be furnished the recipients of such products or substances.

h. Unclassified material. - Unclassified material should not be marked UNCLASSIFIED, unless it is essential to convey to a recipient of such material that it has been examined specifically with the view of imposing a classification and that it has been determined to be unclassified.

i. Material disseminated outside the Department. - When classified information is furnished to authorized persons outside the Department, the following notation, in addition to the assigned classification markings, shall be placed on the document, on the material, on its container, or, when as indicated in sub-paragraph g above, marking is impracticable, on the written notification of its assigned classification:

> "This material contains information affecting the national security of the Philippines, the transmission or revelation of which in any manner to unauthorized persons is punishable under the Revised Penal Code and the Espionage Act (CA Nr 616)."

28. Additional Markings. -

a. All pages of unbound TOP SECRET and SECRET documents shall be marked with the following: (COPY _____ OF _____ COPIES)
(PAGE _____ OF _____ PAGES)

b. All bound TOP SECRET and SECRET matter shall be marked on the front cover as follows: (COPY ____ OF ____ COPIES)

Section VII

CONTROL OF CLASSIFIED MATTER

29. Custody and accounting of classified matter. - Heads of Departments handling classified matter shall issue orders designating their respective custodians of classified matter. Custodians shall -

a. Store all classified matter.

b. Maintain a registry of classified matter showing all classified matter received and to whom transmitted.

c. Maintain a current roster of persons authorized access to classified matter for each classification in the office.

d. Insure physical security for classified matter.

e. Conduct an inventory of all TOP SECRET matter as specified in paragraph 7.

f. Upon his relief, account for all TOP SECRET and SECRET matter by inventory and transmit the same to his successor.

30. Unauthorized keeping of private records. - All government personnel are prohibited from keeping private records, diaries, or papers containing statements of facts or opinions, either official or personal, concerning matters which are related to or which affect national interest or security. Also prohibited are the collection of souvenirs or obtaining for personal use whatsoever any matter classified in the interest of national security.

31. Dissemination. - Dissemination of classified matter shall be restricted to properly cleared persons whose official duties require knowledge or possession thereof. Responsibility for the determination of "need-to-know" rests upon both each individual, who has possession, knowledge or command control of the information involved, and the recipient.

32. Discussion involving classified matter. -

a. Indiscreet discussions or conversation involving classified matter shall not be engaged in within the presence of or with unauthorized persons.

b. When a lecture, address or informal talk to a group includes classified matter, the speaker shall announce the classification at the beginning and end of the period.

e. All personnel leaving the Government Service shall be warned against unlawful disclosures of classified matter.

33. Disclosure to other Departments of classified information originating from another Department. - Classified matter originating from another Department shall not be disseminated to other Departments without the consent of the originating Department.

34. Release of classified matter outside a Department. -

a. General Policy. - No person in the Government shall convey orally, visually or by written communication any classified matter outside his own Department unless such disclosure has been processed and cleared by the Department Head or his authorized representative.

b. Release of classified matter to Congress. -

(1) Government personnel, when giving oral testimony before Congressional Committees involving classified matter, shall advise the committee of the classification thereof. Government personnel called upon to testify shall obtain necessary and prior instruction from his Department Head concerning disclosure.

(2) When Congressional members visit Government offices, Department Heads are authorized to release classified matter which is deemed an adequate response to an inquiry provided that it is required in the performance of official functions.

c. Disclosure to foreign governments or nationals. - Classified matter may be released to foreign governments or nationals of countries having defense obligations with the Philippines, in accordance with sub-paragraph 34a above. The release shall be made only after assurance by the requesting foreign agency or national that:

(1) Its use shall be solely for the purpose for which the classified matter is requested.

(2) It shall be treated or handled in accordance with the classification categories of the originating office.

(3) Handling shall be made by security-cleared personnel.

(4) Reproduction and dissemination shall not be made without the consent of the Department Head.

d. Disclosure of classified matter for publication. - Classified matter shall be released for public consumption only upon the consent of the Department Head or his authorized representative. However, in instances where there is a demand or need for releasing classified information, extreme care and caution must be exercised to analyze in detail the contents of the classified matter before release. Normally, all information are released through Public Information Officers. Public Information Officers should be assisted in the analysis of classified information by the Security Officer.

e. Disclosure through conferences and meetings. -

(1) Disclosure of classified matter in conferences

and other gatherings which include personnel outside the Department shall be in accordance with sub-paragraph 34a above. In conducting conferences involving classified information, the following data should be requested from each participant:

(a) Name and designation or position of participant.

(b) Address of participant.

(c) Signature of participant.

(2) Physical security of the conference room should be assured. Sponsoring agencies shall observe, among other things, the following:

(a) Arrangements for admission of those persons authorized to attend. All individuals must produce positive identification.

(b) Arrangements for protection of classified matter handled during the meeting.

(c) Control of signal equipment, notes and memoranda.

(d) Provision of adequate guards.

35. Removal of classified matter from offices for official use. -

a. Classified matter shall not be removed from offices for the purpose of working on such matter at night or for other purposes involving personal convenience. When necessity requires such removal, Department Heads through the Security Officer shall insure that adequate controls are established as follows:

(1) An appropriate authority specifically designated by the Department Head shall authorize each removal only after insuring that adequate security for the material can be provided.

(2) Storage safeguards shall be strictly observed.

b. Department Heads shall maintain a temporary record in whatever appropriate form of all classified matter removed from their facilities or installations to insure that they are accounted for.

36. Compromise or loss of classified matter. -

a. Any person who becomes aware of the disclosure, or the possibility of disclosure, of classified matter to any unauthorized person, or the loss of a classified document, shall immediately notify by the fastest means available the:

(1) Security Officer of the Department having primary interest (normally the originator), and the

(2) Department Head of the individual having custody.

b. The Department Head of the individual having custody shall cause an investigation to be made. This

investigation will fix individual responsibility for the compromise or possible compromise of TOP SECRET and SECRET matter and, when it can not be established, will fix responsibility on the appropriate officer who allowed the existence of inadequate or insecure conditions, which led to the compromise or possible compromise. In every case, the Head of the Department concerned shall take positive action to correct deficiencies and prevent recurrences, including appropriate disciplinary action and/or criminal prosecution against responsible individuals.

Section VIII

REGRADING AND DECLASSIFICATION

37. Responsibility for regrading. -

a. Each Department Head shall keep under continuing review all classified information in his custody, or of primary interest to him, and will initiate downgrading or declassifying action as soon as conditions warrant.

b. In obvious cases of overclassification or underclassification, higher authority may adjust the classification without referral to the originator, except to notify the originator of the change of classification. The originator will then take the action specified in paragraph 40.

38. Downgrading or declassification. -

a. Originators or letters of transmittal or other covering documents, classified solely or partially because of classified inclosures, shall place on such documents a notation substantially as follows:

"REGRADED UNCLASSIFIED (or appropriate classification) WHEN SEPARATED FROM CLASSIFIED INCLOSURES."

b. For classification purposes, indorsements and numbered comments or routing slips will be handled as separate documents.

c. Holders of classified matter may downgrade or declassify them when circumstances do not warrant retention in the original classification, provided the consent of the appropriate classification authority has been obtained. The downgrading or declassification of extracts from or paraphrases of classified documents also require the consent of the appropriate classification authority. Material which has been classified by a friendly foreign nation or international organization or another Department of the Philippine Government will be downgraded or declassified only with the consent of the originator.

39. Regrading. - If the recipient of classified matter believes that it has been classified too highly, he may request the originator for its downgrading or declassification. If the recipient of unclassified material believes that it should be classified or if the recipient of classified material believes that its classification is not sufficiently protective, the recipient may request the originator to classify the material or upgrade it.

40. Notification of change of classification. -

a. The official taking action to declassify, downgrade or upgrade classified material shall notify all addressees to whom the material was originally transmitted. Officials providing additional distribution (other than initial) of classified material should notify all recipients to whom the additional distribution was furnished of the regrading action required.

b. When downgrading a document in part, the originating Department shall notify recipients as to the new classification of separate chapters, sections, paragraphs or other appropriate subdivisions.

41. Marking of regraded documents. -

a. Authority annotation - Whenever classified matter is declassified, downgraded or upgraded, each copy of the material shall be marked or stamped on the front cover or on the first page, if the document has no cover, with a notice in the following manner:

(1) REGRADED _____ (enter new classification), BY AUTHORITY OF _____ (enter title or position of official authorized to make the change), BY _____ (enter name, grade and organization of the official making the change), ON _____ (enter the date on which the change was made).

b. Classification markings - Regraded documents and material shall be re-stamped or re-marked (not typed) as prescribed in paragraph 27 above and the old classification markings lined through. If the document is declassified, the classification markings on the outside of the front and back covers, title page and first and back pages of the text should be lined through. Prints of motion picture films shall show regrading or declassification action on leaders attached between the plain leader and first title frame.

c. Documents on file - When classified documents on file can not be immediately regraded for obvious reasons, such as the inability to screen a large volume of files to locate the document, the Department Head concerned may establish a system in which individual documents are regraded when charged out of the file for use or screened for regrading purposes, whichever occurs first. In cases requiring upgrading, material shall be given storage safeguards required by the new classification.

Section IX

TRANSMISSION OF CLASSIFIED MATTER

42. Classified document receipts. -

a. Transmission of TOP SECRET and SECRET documents shall be covered by a receipt system (ANNEX B). Transmission of CONFIDENTIAL documents may be covered by a receipt system when required by the sender.

b. The receipt form will identify the addressor, addressees and the document, but should not contain classified

information. It shall be signed by the recipient and returned to the sender. The name of the recipient shall be printed, stamped or typed on the form.

43. Cover Sheets. - Classified documents shall be covered with cover sheets as follows:

For TOP SECRET (ANNEX C)	- 8" x 13" white paper lined with 1/2" green border.
For SECRET (ANNEX D)	- 8" x 13" white paper lined with 1/2" red border.
For CONFIDENTIAL (ANNEX E)	- 8" x 13" white paper lined with 1/2" blue border.

Security classification and instructions are printed on the front page of the cover sheet. The back page is designed to show a record of transmission of the document it will cover.

a. All classified documents (CONFIDENTIAL and up), from the moment they are initiated, shall be covered by appropriate cover sheets, which shall stay with such documents until both are authorized for destruction.

b. When a TOP SECRET or SECRET document is reproduced, the reproduced copies shall be provided with new cover sheets and the "Record of Transmission" on the back page shall record only those personnel who handled each copy from the moment of its reproduction.

c. Cover sheets prescribed by this Executive Order shall be used only for classified documents transmitted among the various Departments of the National Government.

44. Preparation of classified matter for transmission outside a Department. -

a. Classified documents for transmission by Philippine registered mail or diplomatic pouch shall be prepared as follows:

(1) The documents shall be inclosed in two opaque envelopes or covers.

(2) A receipt shall be inclosed with the document as appropriate.

(3) The inner envelope or cover shall be addressed and sealed with sealing wax. The return adress should likewise be written in the inner envelope.

(4) The classification on the front and back of the inner envelope shall be marked in such a way that the markings will be easily seen when the outer cover is removed. Special markings required shall be placed on the front of the inner envelope.

(5) The inner envelope shall be inclosed in the opaque outer envelope or cover. The classification marking of the inner envelope must not be detectable through the outer envelope.

(6) The outer envelope with the inner envelope will then be forwarded. Classification or other special markings shall not appear on the outer envelope.

b. Classified documents for transmission through specifically authorized couriers shall be prepared as follows:

(1) The documents shall be inclosed in an opaque sealed envelope.

(2) The document shall be covered by a receipt as appropriate.

(3) The envelope shall be addressed and provided with a return address. No classification or other markings shall appear on the envelope.

45. Transmission within a Department. - Preparation of classified matter for transmission within a Department shall be governed by regulations issued by the Head of the Department.

Section X

SECURITY OF CONTAINERS

46. Unlocked containers. -

a. Any person finding a container of classified matter unlocked and unattended shall:

(1) Report such fact immediately to the Head of the Department concerned, or to the Security Officer.

(2) Notify the person responsible for the container and its contents.

(3) Lock the container.

b. When notified that a container of classified matter has been found unlocked and unattended, the individual responsible for the container shall check the contents for visible indications of tampering.

c. Persons who find classified matter out of safes and unattended shall immediately report such fact to the Head of the Department or to the Security Officer.

47. Record of locking and unlocking containers. - Officers responsible for TOP SECRET and SECRET matters shall maintain a record of the time and date the container is locked and unlocked.

48. Changing, recording and disseminating container combinations. -

a. Combinations shall be changed at least once every six (6) months and at such other times as deemed appropriate, and at the earliest practicable time following:

(1) The loss or possible compromise of the safe combination.

(2) The discharge, suspension or reassignment of any person having knowledge of the combination.

(3) The receipt of a container.

b. Identification numbers must be obliterated from combination padlocks prior to their use. Three-position dial-type combination padlocks, the combinations of which can be changed in the manner as those of locks built into safes, need not have the manufacturer's identification numbers obliterated.

49. Control of keys. - Keys shall be safeguarded as follows:

a. All keys shall be recorded in a control register and checked periodically.

b. All keys for containers of classified matter when not in use shall be placed in a locked box in the office under the care of a responsible officer.

c. Duplicate keys should be placed in a sealed container and kept in a combination safe.

d. The loss of a key must be reported to the Head of the Department or to the Security Officer.

e. Department Heads shall institute additional measures to safeguard keys appropriate to their respective offices.

Section XI

MISCELLANEOUS

50. Special procedures for safeguarding certain documents from foreign nationals. -

a. Classified information which should be withheld from foreign nationals shall be stamped or marked with a special handling notice as follows:

> SPECIAL HANDLING REQUIRED. RELEASE TO FOREIGN NATIONALS NOT AUTHORIZED EXCEPT _____ (enter "None" or names of representatives of foreign nations specifically authorized to have access to the document) BY AUTHORITY OF _____ (enter title or position of official authorized to determine which foreign nationals may have access to the document) DATE _____ (enter date).

51. Classified matter in the possession of individuals on travel orders. -

a. An individual on travel orders who is authorized to have in his possession classified matter shall safeguard such matter by one of the following methods:

(1) By contacting and availing of the storage facilities of the nearest respective field or branch office, or Armed Forces installation; or

(2) By keeping the matter under personal physical control at all times.

b. Personnel on travel status shall not carry classified matter across international borders where the classified matter may be liable to scrutiny by customs inspectors or other unauthorized individuals. Such matter should be sent in advance by diplomatic pouch or diplomatic courier only.

52. Emergency destruction. -

a. Plans. - Department Heads shall provide for emergency destruction or safe removal of all classified matter under their jurisdiction should civil disturbances, disaster or enemy action require such action.

b. Aboard airplane or ship. - If a craft carrying classified matter is forced down, stranded or shipwrecked on unfriendly territory or on neutral territory where capture appears imminent or, under any other circumstances where it appears unlikely that the classified matter can properly be protected, such matter shall be destroyed in any manner that will render recognition impossible, preferably by burning.

53. Security of typewriter ribbons. - Cotton, rayon, paper and silk typewriter ribbons are insecure until typed through at least twice. Insecure ribbons shall be appropriately safeguarded if used to type classified information. Nylon ribbons are secure at all times.

54. Classified waste. - Waste, such as preliminary drafts, notes, dictaphone- or other-type recordings, typewriter ribbons, carbon paper, stencils, stenographic notes, carbon plates, exposed film (developed or undeveloped) and similar items containing classified information shall be disposed of in a manner prescribed for similarly classified matter. Certificate of destruction is not required.

55. Supplementary security regulations. - Department Heads shall publish regulations to supplement this Executive Order to include measures appropriate to their respective Departments as indicated herein and to cover the following general subjects or circumstances:

a. Movement control of organic personnel and visitors within their respective jurisdictions.

b. Security arrangements in dealing with government contractors engaged in projects concerning classified matter.

c. Security measures to safeguard classified information transmitted through electronic communication facilities.

Department Heads shall seek the assistance of the Director, National Intelligence Coordinating Agency or of the Secretary of National Defense in preparing the above supplemental regulations.

56. Security Clearance. - The Head of the Department shall be responsible for the issuance of security clearances in his Department. In this regard he may coordinate directly with the National Intelligence Coordinating Agency or the Department of National Defense.

Section XII

ADMINISTRATIVE LIABILITY

57. Any violation of the provisions of these regulations shall be dealt with administratively by proper authorities. Said administrative proceeding shall be without prejudice to any criminal prosecution if the violation constitutes an offense under the provisions of the Revised Penal Code or any other penal law. The unauthorized publication of any classified information shall be deemed a violation of these regulations by the parties responsible therefor.

All executive orders, proclamations or circulars inconsistent herewith are hereby revoked.

By authority of the President:

CALIXTO O. ZALDIVAR
Acting Executive Secretary

Manila, August 14, 1964

ANNEX "A"

CERTIFICATE OF DESTRUCTION OF CLASSIFIED RECORDS — OFFICE

DATE OF DOCUMENT	CLASSIFICATION	RECEIPT IDENTIFICATION NO.	REFERENCE NO (SUBJECT)	ORIGINATING AGENCY	ADDRESS	AUTHORITY FOR DESTRUCTION

I CERTIFY THAT I HAVE THIS DATE RECEIVED FOR DESTRUCTION THE DOCUMENTS LISTED ABOVE.	DATE	SIGNATURE OF CUSTODIAN:
I CERTIFY THAT I HAVE THIS DATE DESTROYED IN ACCORDANCE WITH SECURITY REGULATIONS THE DOCUMENTS LISTED ABOVE.	DATE	SIGNATURE OF PERSON MAKING DESTRUCTION:
I CERTIFY THAT I HAVE THIS DATE WITNESSED THE DESTRUCTION OF THE ABOVE LISTED DOCUMENTS.	DATE	SIGNATURE OF WITNESSING OFFICER:

ANNEX "Ø"

OFFICIAL RECEIPT FOR CLASSIFIED MATTER

FROM : _____

_____

) : _____

_____

CONTROL NO. _____

FILE : _____

NO.: _____ of _____ Copies

I acknowledge to have received on this _____ day of _____ 196_____ at _____ Hr the following classified documents:

Brief Description	Classification

NOTE : _____

_____

_____

_____

_____

(SIGNATURE)

FULL NAME & DESIGNATION IN PRINT

OFFICE TEL. NO. _____

TOP SECRET

(Unclassified if not covering Top Secret Document)

THIS IS A COVER SHEET

WARNING:

THE UNAUTHORIZED DISCLOSURE OF THE INFORMATION CONTAINED IN ATTACHED DOCUMENT WOULD CAUSE EXCEPTIONALLY GRAVE DAMAGE OR DANGER TO THE NATION, EITHER POLITICALLY, ECONOMICALLY OR FROM A SECURITY OR MILITARY STANDPOINT.

RESPONSIBILITY OF PERSONS HANDLING ATTACHED DOCUMENT(S)

1. Do not leave the document(s) unattended except when properly secured.

2. Transfer the document(s) only to persons who need to know and who possess the required security clearance.

3. Obtain a receipt whenever relinquishing control of the document(s).

STORAGE:

Safe or its approved equivalent

REPRODUCTION:

The document may be copied, extracted or reproduced only when classifying authority has authorized such action. Reproduction should be under the supervision of an authorised officer/official.

DISPOSITION:

This cover sheet should be treated as part of the document to which it is attached and should be included when the document is permanently filed.

REQUIREMENT:

Anybody who handled, read or acted on attached document(s) shall sign in the appropriate space provided for in record of transmission on the other side of this cover sheet.

TOP SECRET

(Unclassified if not covering document)

RECORD OF TRANSMISSION OF CLASSIFIED DOCUMENT

Office of origin _____ DATE _____

SUBJECT OF CLASSIFIED DOCUMENT

Copy Nr_____ Nr of pages _____

PERSONNEL WHO HAVE HANDLED, READ AND/OR ACTED ON THE DOCUMENT

Signature over Printed name	Assignment	Date Rec'd	& Time Rel'd

(Unclassified if not covering document)

RECORD OF TRANSMISSION OF CLASSIFIED DOCUMENT

Office of origin _____ DATE _____

SUBJECT OF CLASSIFIED DOCUMENT

Copy Nr_____ Nr of pages _____

PERSONNEL WHO HAVE HANDLED, READ AND/OR ACTED ON THE DOCUMENT

Signature over Printed name	Assignment	Date Rec'd	& Time Rel'd

SECRET

(Unclassified if not covering Secret Document)

THIS IS A COVER SHEET

WARNING:

THE UNAUTHORIZED DISCLOSURE OF THE INFORMATION CONTAINED IN ATTACHED DOCUMENT(S) WOULD ENDANGER NATIONAL SECURITY, CAUSE SERIOUS INJURY TO THE INTEREST OR PRESTIGE OF THE NATION OR OF ANY GOVERNMENTAL ACTIVITY THEREOF OR WOULD BE OF GREAT ADVANTAGE TO A FOREIGN NATION.

RESPONSIBILITY OF PERSONS HANDLING THE ATTACHED DOCUMENT(S):

1. Do not leave the document(s) unattended except when properly secured.
2. Transfer the document(s) only to persons who need to know and who possess the required security clearance.
3. Obtain a receipt whenever relinquishing control of the document(s).

STORAGE:

Safe or its approved equivalent

REPRODUCTION:

Copies should not be made without consent of the originating agency.

DISPOSITION:

This cover sheet should be treated as part of the document to which it is attached and should be included when the document is permanently filed.

REQUIREMENT:

Anybody who handles [illegible] attached document(s) shall sign in the appropriate space provided for in record of transmission on the other side of this cover sheet.

SECRET

CONFIDENTIAL

(Unclassified if not covering Confidential document)

THIS IS A COVER SHEET

WARNING:

THE UNAUTHORIZED DISCLOSURE OF THE INFORMATION CONTAINED IN THE ATTACHED DOCUMENT(S) WHILE NOT ENDANGERING NATIONAL SECURITY WOULD BE PREJUDICIAL TO THE INTEREST OR PRESTIGE OF THE NATION, ANY GOVERNMENTAL ACTIVITY, OR WOULD CAUSE ADMINISTRATIVE EMBARRASSMENT OR UNWARRANTED INJURY TO AN INDIVIDUAL, OR WOULD BE OF ADVANTAGE TO A FOREIGN NATION.

RESPONSIBILITY OF PERSONS HANDLING THE ATTACHED DOCUMENT(S):

1. Do not leave the document(s) unattended except when properly secured.
2. Transfer the document(s) only to persons who need to know and who possess the required security clearance.
3. If so required obtain a receipt whenever relinquishing control of the document(s).

STORAGE:

Safe or filing cabinet with iron bar & combination padlock

REPRODUCTION:

Copies may be made of these documents except when the originating office has specifically stated that no copy shall be made without prior authority.

DISPOSITION:

This cover sheet need not be included when the original document is permanently filed.

CONFIDENTIAL

TABLE OF CONTENTS

		Paragraph	Page
SECTION I	GENERAL		
	Classification categories	1	1
	Definition of terms	2	1- 2
	Security Officers	3	2
SECTION II	TOP SECRET MATTER		
	Definition.	4	2- 3
	Classification Authority.	5	3
	Reproduction.	6	3
	Inventory	7	3
	Transmission.	8	3- 4
	Storage	9	4
	Destruction	10	4
SECTION III	SECRET MATTER		
	Definition.	11	4- 5
	Classification Authority.	12	5
	Reproduction.	13	5
	Transmission.	14	5
	Storage	15	5- 6
	Destruction	16	6
SECTION IV	CONFIDENTIAL MATTER		
	Definition.	17	6
	Classification Authority.	18	7
	Reproduction.	19	7
	Transmission.	20	7
	Storage	21	7
	Destruction	22	7
SECTION V	RESTRICTED MATTER		
	Definition.	23	7
	Authority to Classify, Reproduction, Dissemination and Destruction . .	24	7
SECTION VI	CLASSIFYING AND MARKING		
	General	25	7
	Rules for classification.	26	7- 8
	Classification marking.	27	8- 9
	Additional Markings	28	10
SECTION VII	CONTROL OF CLASSIFIED MATTER		
	Custody and accounting of classified matter.	29	10
	Unauthorized keeping of private records	30	10
	Dissemination	31	10
	Discussion involving classified matter	32	10-11
	Disclosure to other Departments of classified information originating from another Department	33	11
	Release of classified matter outside a Department.	34	11-12
	Removal of classified matter from offices for official use.	35	12
	Compromise or loss of classified matter.	36	12-13
SECTION VIII	REGRADING AND DECLASSIFICATION		
	Responsibility for regrading. . . .	37	13
	Downgrading or declassification . .	38	13

	Regrading	39	13
	Notification of change of classification	40	14
	Marking of regraded documents . . .	41	14
SECTION IX	TRANSMISSION OF CLASSIFIED MATTER		
	Classified document receipts . . .	42	14-15
	Cover Sheets	43	15
	Preparation of classified matter for transmission outside a Department	44	15-16
	Transmission within a Department .	45	16
SECTION X	SECURITY OF CONTAINERS		
	Unlocked containers	46	16
	Record of locking and unlocking containers	47	16
	Changing, recording and disseminating container combinations	48	16-17
	Control of keys	49	17
SECTION XI	MISCELLANEOUS		
	Special procedures for safeguarding certain documents from foreign nationals	50	17
	Classified matter in the possession of individuals on travel orders .	51	17-18
	Emergency destruction	52	18
	Security of typewriter ribbons . .	53	18
	Classified waste	54	18
	Supplementary security regulations.	55	18
	Security Clearance	56	18
SECTION XII	ADMINISTRATIVE LIABILITY	57	19

	Regrading	39	13
	Notification of change of classification	40	14
	Marking of regraded documents . . .	41	14
SECTION IX	TRANSMISSION OF CLASSIFIED MATTER		
	Classified document receipts . . .	42	14-15
	Cover Sheets	43	15
	Preparation of classified matter for transmission outside a Department	44	15-16
	Transmission within a Department .	45	16
SECTION X	SECURITY OF CONTAINERS		
	Unlocked containers	46	16
	Record of locking and unlocking containers	47	16
	Changing, recording and disseminating container combinations	48	16-17
	Control of keys	49	17
SECTION XI	MISCELLANEOUS		
	Special procedures for safeguarding certain documents from foreign nationals	50	17
	Classified matter in the possession of individuals on travel orders .	51	17-18
	Emergency destruction	52	18
	Security of typewriter ribbons . .	53	18
	Classified waste	54	18
	Supplementary security regulations.	55	18
	Security Clearance	56	18
SECTION XII	ADMINISTRATIVE LIABILITY	57	19

OFFICE OF THE PRESIDENT
OF THE PHILIPPINES

MEMORANDUM CIRCULAR NO. 196

AMENDING MEMORANDUM CIRCULAR 78 DATED AUGUST 14, 1964, ENTITLED "PROMULGATING RULES GOVERNING SECURITY OF CLASSIFIED MATTER IN GOVERNMENT OFFICES."

1. A new section, to be known as Section XII, is hereby inserted between Sections XI and XII of Memorandum Circular No. 78 dated August 14, 1964, providing security of classified matter in government offices, which reads as follows:

"SECTION XII

"COMMUNICATION SECURITY

"57. Communication Security

a. Definition – Communication Security is the protection resulting from the application of various measures which prevent or delay the enemy or unauthorized persons in gaining information through our communications. It includes Transmission, Cryptographic and Physical security.

b. Rules governing Communication Security do not in themselves guarantee security, and they do not attempt to meet every conceivable situation. Communication Security rules are a means, not an end in themselves.

c. Department Heads are responsible for the maintenance of communication security and for the promulgation of additional

directive a may be necessary to insure proper communication security control within their jurisdiction.

d. All communication personnel should have an appreciation of the basic principles of communication security since the neglect of a single aspect of communication security may result in compromise.

“58. Communication Security Officer:

a. A properly trained and cleared Communication Security Officer shall be appointed in every Department of the Government handling cryptographic communication.

“59 Responsibilities/Duties of the Communication Security Officer:

a. Responsible for the selection and training of cleared communication personnel to perform crypto duties.

b. Responsible for the operations and maintenance of the cryptocenter.

c. Conduct periodic inspection of the cryptocenter to ascertain that crypto materials are properly handled and accounted for and that all directives concerning crypto-operations are strictly observed.

d. Designate a custodian for crypto-matepials,

e. Publish an emergency destruction plan for classified materials.

f. Recommend measures to improve transmission, cryptographic and physical security.

g. Conduct investigation in case of less or compromise of crypto-materials in accordance with paragraph 36 above.

“60. Transmission Security:

a. Definition – Transmission Security is that component of communication security which results from all measures designed to protect transmission from interception, traffic analysis and imitative deception.

b. Communication personnel shall select the means most appropriate to accomplish the delivery of message in accordance with the specified precedence and security requirements.

c. All classified messages within the Government service which are transmitted electrically should be encoded, enciphered and/or encrypted.

d. All classified messages sent by commercial means shall be encoded, enciphered and/or encrypted.

e. No classified message shall be transmitted over a telephone system not equipped with security device.

f. The transmission by visual means of a classified message in plain language shall be authorized only after careful consideration has been given to the necessity for sending in plain language and to the possibility of interception by unauthorized persons.

g. Radio Operations shall adhere to the use of correct procedures, circuit discipline and authentication system as a security measures against traffic analysis, imitative deception and radio direction finding.

“61. Cryptographic Security:

a. Definition – Cryptographic Security is that component of communication security which results from the provisions of technically sound cryptosystem and their proper use.

b. Message should scrutinized prior to encryption giving particular attention to the security classification, precedence, and to any special handling or routing precautions that may be necessary.

c. Messages should be completely checked before transmission to insure that the operating instructions pertaining to the system used have been followed and that the encrypted text is decryptable.

“62. Physical Security:

a. Definition – Physical Security is that component of communication security which results from measures necessary to safeguard classified communication equipment and material from access thereto by unauthorized persons.

b. Physical security measures include handling of classifies materials, i.e., storage, accounting and destruction.”

2. Section XII of the same circular shall hereafter be known as Section XIII, and Item 57 as Item 63.

By authority of the President:
(SGD.) RAFAEL M. SALAS
Executive Secretary

Manila, July 19, 1968.

S. No. 2965
H. No. 4115

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

(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.

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, which 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).

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 be processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided, further,* That adequate safeguards are guaranteed by said laws authorizing their processing.

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.

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 be 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.

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 that 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.

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.

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.

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 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).

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 he 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 abovementioned 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 be applied.

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

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.

Approved,

FELICIANO BELMONTE JR.
Speaker of the House of Representatives

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.

MARILYN B. BARUA-YAP
Secretary General
House of Representatives

EMMA LIRIO-REYES
Secretary of the Senate

Approved: AUG 15 2012

BENIGNO S. AQUINO III
President of the Philippines

O

ANNEX E
DETAILED FOI REQUEST PROCESS

STEP I – PAO, AFP (FRO) Receives Request (1 Day)

- Receive Request
  - Stamp received
  - Provide copy to requestor
  - Log details on FOI tracker
- Initial evaluation
  - Completeness of request
  - Intent of request
  - Availability of the information

If ***denied***:
• Communicate denial to requesting party

If it ***passed the evaluation***:
• Forward to COU

STEP II – Chief, Admin Division (COU) Clarifies, Locates, & Reviews FOI; Request Security Clearance (10 Days)

- Cognizant Office/Unit (COU) receives endorsed request
- Forward to OJ2 for security clearance, if necessary
- Review request and prepare recommendations for the FDM on the approval or denial of the release of information to the requesting party

Information ***NOT found***:
• Communicate denial to requesting party through FRO

Information ***located***:
• Forward endorsed request, security clearance, and information requested to FDM

If an ***extension of time is required***:
• Communicate extension of time to the requesting party through the FRO

STEP III – CSAFP (FDM) Approves or Denies Release of Information Requested (3 Days)

- FDM shall refer to the guidelines set forth in the AFP FOI Manual and the recommendations provided by the COU in approving or denying the release of information requested

Information ***approved***:
• Communicate approval to the FRO for the release of information to the requesting party

Information ***denied***:
• Communicate denial through the FRO

STEP IV – PAO, AFP (FRO) Communicates Response (1 Day)

- FRO communicates response to the requesting party
- Update FOI tracker and save response

STEP V – Requesting Party Filed an Appeal with the TDCSAFP (CARC) (30 Days)

- The requesting party may file an appeal with the CARC within 15 days from notice of denial of the FOI Request
- Failure to appeal after the 15-day period shall be deemed a waiver of the right to appeal
- The CARC, through its FOI Appeals and Review Subcommittee (FARS), shall review, evaluate, and recommend approval or denial of the appeal to CSAFP within 30 days

Information ***approved***:
• Communicate approval to the FRO

Information ***denied***:
• Communicate denial through the FRO

ANNEX F

FOI REQUEST FORM

Name (Pangalan):
Address (Tirahan):
Contact No. (Mobile, Telephone, E-mail, & etc.):
Office/School Address (Lokasyon ng Opisina O Eskwelahan):
Age (Edad):
Gender (Kasarian):
Date of Request (Petsa ng Paghingi ng Impormasyon):
Please state the documents or information you are looking for. (Pakilahad po ang dokumento o impormasyon na inyong hinahanap.)
Please state the covered period of the said documents/information. (Pakilahad po ang panahong saklaw ng nasabing dokumento o impormasyon.)
Please adequately describe your purpose for securing these documents / information. (Pakilarawan po ng malinaw ang inyong layunin sa paghingi ng nasabing dokumento o impormasyon.)
Acknowledgment of Receipt of Document **(Pagkilala ng Pagtanggapng Dokumento)** **Name (Pangalan): _____** **Date & Time (Petsa at Oras): _____** **Lagda (Signature): _____**

Terms of Use: The requested information or document provided shall not be used: (a) for any purpose other than what is stated in the "FOI Request Form"; (b) for any purpose that is contrary to law, public policy, public order, morals, or good customs; and (c) reproduced for any commercial use. Any violation to the said Terms of Use may subject the requesting party to legal actions and/or penalties as may be provided by law.

Mga Tuntunin ng Paggamit: Anumang impormasyon o dokumentong ibinigay ay hindi maaring gagamitin: (a) para sa anumang layunin maliban sa kung ano ang nakasaad sa nilagdaang "FOI Request Form"; (b) para sa anumang layunin na salungat sa batas, pampublikong patakaran, pampublikong kaayusan, moralidad, o mabuting kaugalian; at (c) para sa anumang komersyal na paggamit. Anumang paglabag sa nasabing mga Tuntunin ng Paggamit ay may karampatang legal na aksyon at/o parusang naaayon sa batas.

ANNEX G

FOI APPEAL TEMPLATE

[Date]

Armed Forces of the Philippines

Dear Sir/Ma'am,

I submitted a request for information dated _____ asking for _____. Attached is a copy of the said request **(Tab A)**.

On _____, I received a notice **(Tab B)** denying the abovementioned request for the following reason: _____.

I would like to appeal this denial on the following ground/s: _____ _____ _____.

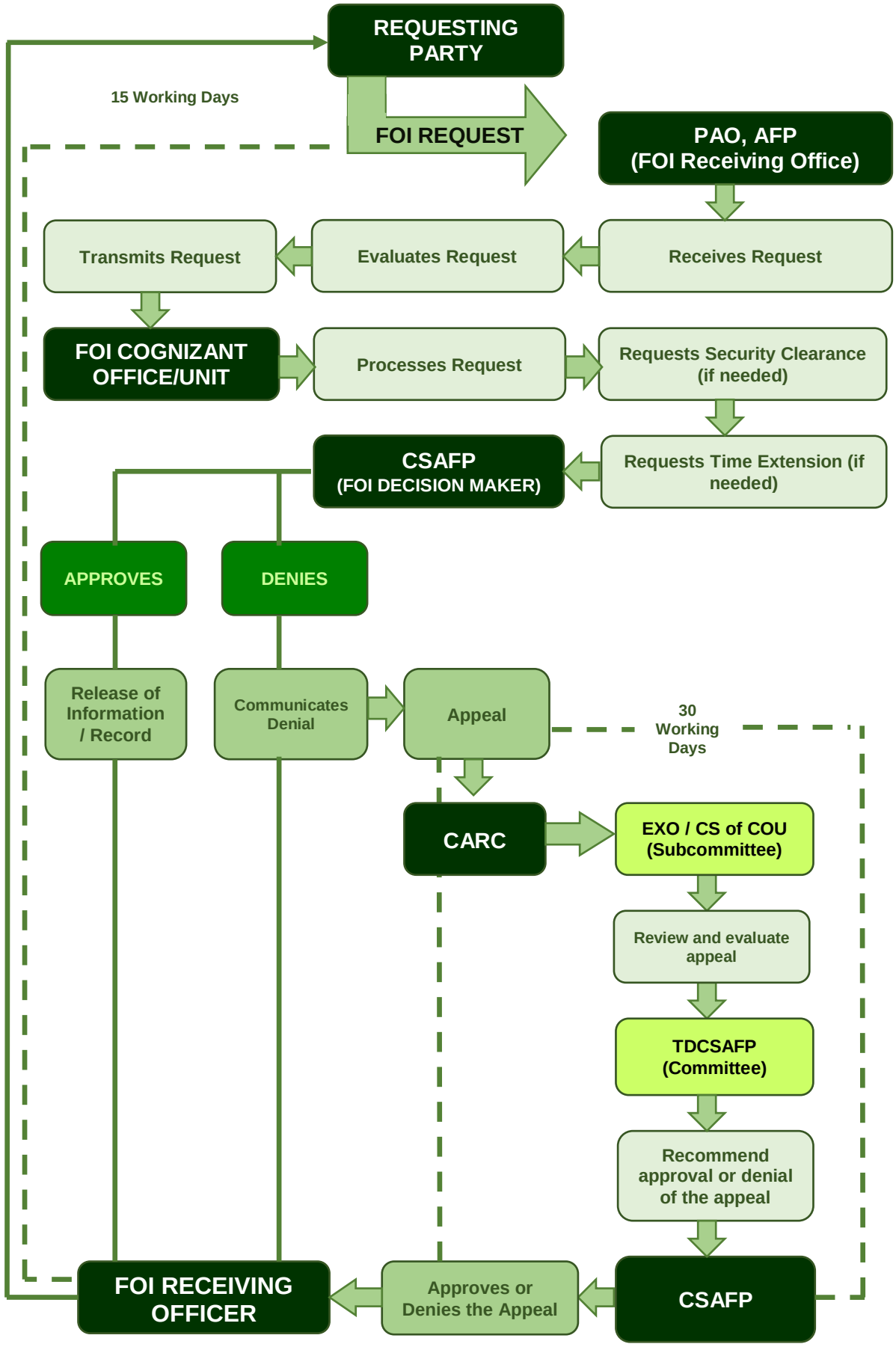
This appeal is being filed within fifteen (15) days from receipt of the notice of denial.

Thank you.

Respectfully,

Requesting Party

ANNEX H
FOI FLOW CHART



NOTE:
- - - number of working days