



MAY 28 2018

Memorandum Circular No. 003 P
Series of 2018

SUBJECT : Implementation of NAMRIA Privacy Manual

In the interest of the service and pursuant to Republic Act No. 10173 otherwise known as the Data Privacy Act of 2012, the "NAMRIA Privacy Manual" is hereby implemented effective immediately.

The Privacy Manual outlines NAMRIA's data protection and privacy measures and serves as a guide to all stakeholders in the exercise of their rights under DPA.

For guidance and compliance.


Usec. PETER N. TIANGCO, PhD
Administrator



ISO 9001:2008 CERTIFIED FOR MAPPING AND GEOSPATIAL INFORMATION MANAGEMENT
NAMRIA OFFICES:
Main : Lawton Avenue, Fort Bonifacio, 1634 Taguig City, Philippines Tel. No.: (632) 810-4831 to 41
Branch : 421 Barraca St. San Nicolas, 1010 Manila, Philippines, Tel. No. (632) 241-3494 to 98
www.namria.gov.ph



Republic of the Philippines
Department of Environment and Natural Resources
NATIONAL MAPPING AND RESOURCE INFORMATION AUTHORITY
Lawton Ave., Fort Bonifacio, Taguig City 1634

STAFF COVER MEMORANDUM

FOR : **The Administrator**

FROM : The Director
Support Services Branch (SSB)

SUBJECT : **Privacy Manual**

DATE : 30 April 2018

May we request your approval and signature on the attached Privacy Manual which was drafted during a series of seminar-workshops and coaching sessions, including the conduct of a Privacy Impact Assessment (PIA), held last February-March 2018. The activities were conducted in line with the agency's effort to implement a Privacy Management Program.

We have already complied with the first two (out of five) pillars of the Data Privacy Accountability and Compliance, which are the Appointment of a Data Protection Officer and Conduct of PIA. The manual is our third commitment to safeguard personal data and implement the Data Protection Act of 2012 (DPA).

The Privacy Manual outlines NAMRIA's data protection and privacy measures and serves as a guide to all stakeholders in the exercise of their rights under DPA.

Upon approval, the manual will be packaged by the Geospatial Information Services Division for the information of NAMRIA stakeholders and dissemination.


FEBRINA E. DAMASO



NAMRIA OFFICES:
Main : Lawton Avenue, Fort Bonifacio, 1634 Taguig City, Philippines Tel. No.: (632) 810-4831 to 41
Branch : 421 Barraca St. San Nicolas, 1010 Manila, Philippines, Tel. No. (632) 241-3494 to 98
www.namria.gov.ph



National Mapping and Resource Information Authority

PRIVACY MANUAL

All Rights Reserved. 2018.

MESSAGE FROM THE ADMINISTRATOR

Personal data are extensively used in individual, professional, and business transactions. What is more, the fast and incessant shifts in information, communication, and geolocation technologies have supported, facilitated, and enabled the free flow and exchange of these data.

Government agencies are duty-bound to safeguard personal data within their custody and to respect the data privacy rights of its employees, clients, partners, and stakeholders. The National Mapping and Resource Information Authority (NAMRIA) formulated this Privacy Manual to fulfill these obligations honorably.

The NAMRIA Privacy Manual serves as the agency's framework and guidebook in protecting personal information within its responsibility and promoting personal data privacy. It lays out the policies and procedures that need to be observed and carried out within NAMRIA to ensure the security and confidentiality of personal data.

These protocols cover processing personal data; implementing adequate organizational, physical, and technical security measures to prevent privacy breaches; notifying personal data breach and security incidents; and upholding the rights of data subjects. The Privacy Manual also contains NAMRIA memoranda, confidentiality agreement, and standard forms for references and usage of the agency's personnel.

A pillar of Data Privacy Accountability and Compliance, the NAMRIA Privacy Manual was crafted in accordance with the regulations of the Data Privacy Act of 2012 and the National Privacy Commission. It affirms the commitment of NAMRIA in strengthening the implementation of national laws on privacy and in adhering to international standards in data protection. This commitment is geared towards an organizational culture aware and protective of personal data privacy rights.

I hope that through this Privacy Manual, NAMRIA will earn more trust from its employees, clients, partners, and stakeholders—our data subjects; and that they will gain more confidence in their engagements, transactions, and undertakings with the agency for a geospatially empowered Philippines.



Usec. PETER N. TIANGCO, PhD
Administrator

TABLE OF CONTENTS

Message from the Administrator

NAMRIA Profile

- About NAMRIA
- Core Functions
- Organizational Structure

NAMRIA Privacy Manual

- Acronyms
- Background
- Introduction
- Definition of Terms
- Scope and Limitations
- Processing of Personal Data
 - A. Collection
 - B. Use
 - C. Storage, Retention, and Destruction
 - D. Access
 - E. Disclosure and Sharing
- Security Measures
 - A. Organizational Security Measures
 - 1. Conduct of Privacy Impact Assessment
 - 2. Designation of Data Protection Officer
 - 3. Functions of the DPO and/or Any Other Responsible Personnel with Similar Functions
 - 4. Duty of Confidentiality
 - 5. Review of Privacy Manual
 - B. Physical Security Measures
 - 1. Facility Security Plan
 - 2. Workstation Security
 - 3. Format of Data
 - 4. Storage Type and Location
 - 5. Procedure in Case of Access by Inadvertence
 - 6. General Safeguards and File Maintenance
 - 7. Monitoring and Limitation of Access
 - 8. Modes of Transfer of Personal Data with Third Parties
 - C. Technical Security Measures
 - 1. Access Controls
 - 2. Integrity
 - 3. Encryption
- Breach and Security Incidents

- A. Procedure for Breach Notification
 - 1. Nature of the Breach
 - 2. Personal Data Possibly Involved
 - 3. Measures Taken to Address the Breach
- B. Creation of a Data Breach Response Team
- C. Measures to Prevent and Minimize the Occurrence of Breach and Security Incidents
- D. Procedure for Recovery and Restoration of Personal Data
- E. Documentation and Reporting Procedure of Security Incidents or Personal Data Breach

Rights, Inquiries, and Complaints of Data Subjects

- A. Rights of Data Subjects
- B. Inquiries and Complaints
 - 1. Inquiries
 - 2. Procedure for Personal Data Breach Complaints
- C. Procedures

Separability Clause

Effectivity

Appendices

- A. NAMRIA Records and Disposition Schedule
- B. Confidentiality Agreement
- C. Client Request Form

ABOUT NAMRIA

As provided for in the Department of Environment and Natural Resources (DENR) Administrative Order (DAO) Number (No.) 31, series of 1988, which prescribes the guidelines implementing Section 22 (a) of Executive Order No. 192 dated 10 June 1987, the National Mapping and Resource Information Authority (NAMRIA) is mandated to provide the public with mapmaking services and to act as the central mapping agency, depository, and distribution facility for natural resources data in the form of maps, charts, texts, and statistics.

NAMRIA undertakes and is responsible for integrated surveys, mapping, charting and oceanography, land classification, aerial photography, remote sensing, resource information management, and research development thereof.

CORE FUNCTIONS

- **Geodetic Reference System Development.** NAMRIA is mandated to establish and maintain the Philippine Geodetic Reference System, the primary positioning reference for all surveying and mapping in the country. It is in line with this mandate that the agency is undertaking the modernization of the national geodetic system (NGS) as part of its core initiatives under its vision of building a geospatially-empowered Philippines. The modernization program is aligned with Resolution 69/266 adopted by the United Nations General Assembly dated 26 February 2015, that urges the adoption of and calls for the active participation of member states in the definition of a global geodetic reference frame for sustainable development. The program will upgrade the existing Philippine Reference System of 1992 into a geocentric datum, develop the national vertical datum, and strengthen the awareness of NGS stakeholders and the core competencies of NAMRIA personnel on geodesy.
- **Topographic Base Mapping.** NAMRIA produces topographic maps and derivative maps in various scales, in paper or digital forms. These are used as basic tools and common references in most aspects of governance such as development planning, disaster risk reduction and management (DRRM), and delivery of government services. They are also used by the private sector in investment planning and exploration; by the academic and science communities in research and development activities; and by the general public. Topographic maps are regularly updated using the latest aerial photographs, satellite imageries, and field surveys. Small-scale (1:250,000) and medium-scale (1:50,000) topographic maps generally cover

large areas for macro planning. Large-scale (1:10,000 and 1:4,000 or larger) topographic maps generally cover smaller areas per map sheet but are more accurate and show more detail. NAMRIA likewise produces updated administrative maps in the form of provincial and regional maps.

- **Hydrography, Physical Oceanography and Nautical Charting.** NAMRIA conducts hydrographic and physical oceanographic surveys, and produces nautical charts like berthing, harbor, approach, coastal, general sailing, and overview charts depicting the country's maritime jurisdictions. The agency also publishes predicted tide and current tables, coast pilot book, list of lights, notices to mariners, and other nautical publications. The nautical charts and publications ensure safety in maritime navigation and provide basic information for the management of the maritime space and resources, as well as base data for climate change studies. The charts and hydrographic data are important in complying with the provisions of the United Nations Convention on the Law of the Sea relative to the country's maritime entitlements. Likewise, the nautical publications are required under the Safety of Life at Sea Convention under the International Maritime Organization.
- **Environment and Natural Resource Mapping.** NAMRIA conducts nationwide environment and natural resource assessment and mapping of various thematic geospatial information such as land cover, coastal resources, low-lying areas vulnerable to sea-level rise, tenurial instruments, and upland/forestland population, among others. These fundamental datasets serve as vital inputs in policy formulation, physical and developmental planning, provision of social services, DRRM, and climate change mitigation and adaptation studies at various levels. In addition, the agency continues to provide information on classification of lands of the public domain as well as technical assistance to DENR on the delineation of forestland boundaries to support legislation by Congress of the final limits of forestlands and national parks.
- **Maritime Zones and Boundaries Mapping.** NAMRIA is responsible for the survey and mapping of the country's terrestrial and maritime territories. It delineates the different maritime zones of the archipelago including the Exclusive Economic Zone and continental shelves. It spearheaded the successful defense in 2012 of the country's submission to the United Nations for an extended continental shelf in the Benham Rise Region, now Philippine Rise. It also provides technical support to various government agencies on matters pertaining to maritime boundary delimitation and Law of the Sea issues, as well as to the local government

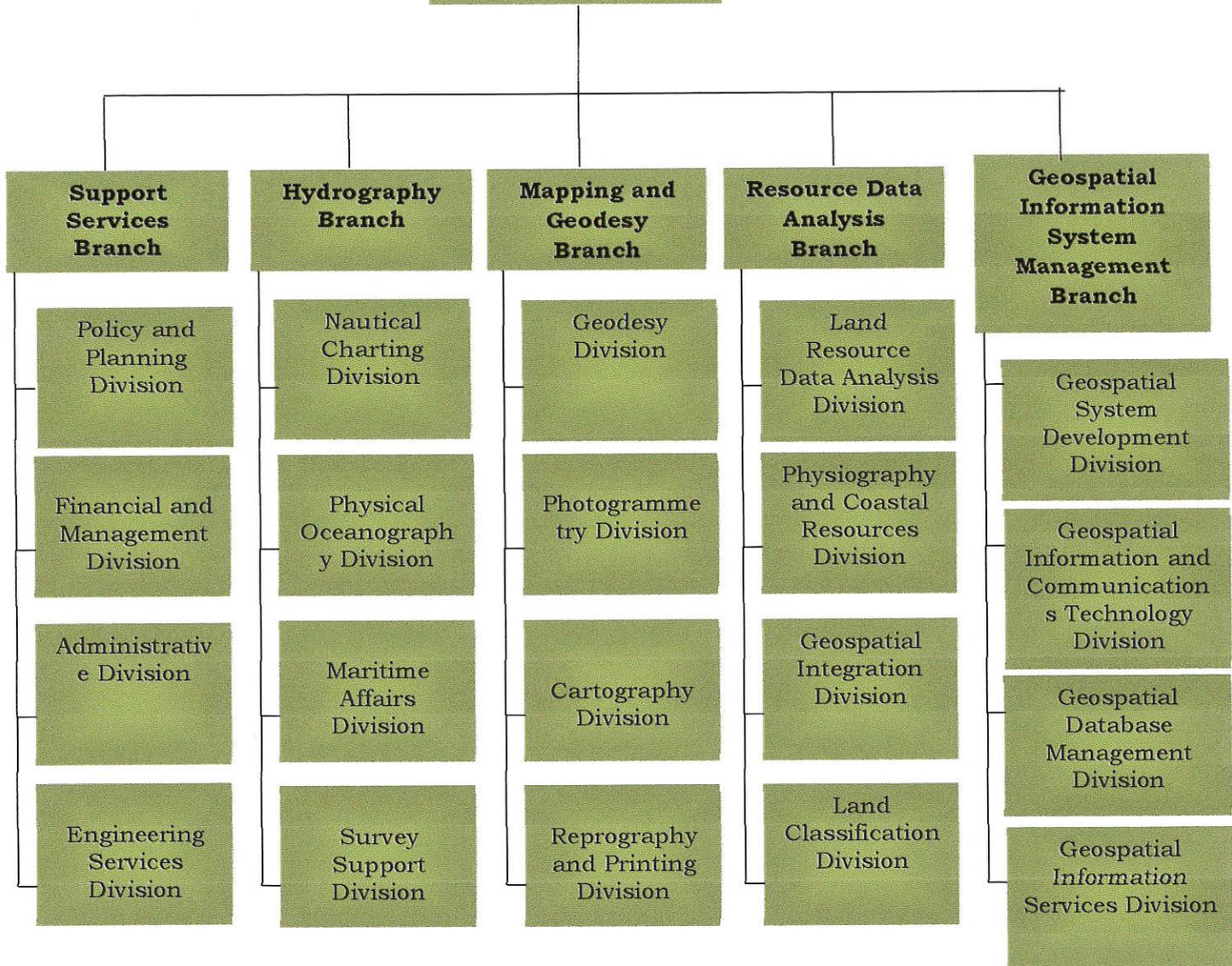
units (LGUs) in the delineation and delimitation of the 15-kilometer municipal water boundaries.

- **Geospatial Information Management and Services.** NAMRIA's geospatial information management and services include information system strategic planning; geospatial databasing; information and web system development; information and communications technology resource and network management; geographic information systems (GIS) project collaboration and technical assistance; GIS trainings; packaging of geospatial information products and services; stakeholder relations and partnership development; information, education, and communication; and customer services. NAMRIA also plays active roles and even acts as lead in local and international programs in the area of geospatial information management and services relevant to DRRM and climate change adaptation. NAMRIA leads in the implementation of the Philippine Spatial Data Infrastructure, which is designed to provide a mechanism for sharing of and access to geospatial information produced and maintained by the various stakeholders and custodians across the country. A major output of the Philippine Spatial Data Infrastructure is the Philippine Geoportal, an application system managed by NAMRIA which serves as a platform for online and open sharing of geospatial information.

ORGANIZATIONAL STRUCTURE

The figure below shows the organizational structure of NAMRIA. The agency is headed by an Administrator assisted by two Deputy Administrators. It is composed of five branches (one support branch and four technical branches), namely: Support Services Branch, Hydrography Branch, Mapping and Geodesy Branch, Resource Data Analysis Branch, and Geospatial Information Systems Management Branch (GISMB). Under each branch are four operational divisions. Each branch is headed by a Director while each Division is headed by a Division Chief.

OFFICE OF THE ADMINISTRATOR



ACRONYMS

COP	Compliance Officer for Privacy
DPA	Data Privacy Act
DPO	Data Protection Officer
DPC	Data Protection Committee
DPS	Data Processing System
DSA	Data Sharing Agreement
IRR	Implementing Rules and Regulations
MSO	Map Sales Office
NAMRIA	National Mapping and Resource Information Authority
NDA	Non-Disclosure Agreement
NPC	National Privacy Commission
PI	Personal Information
PDI	Personal Data Inventory
PIA	Privacy Impact Assessment
PIC	Personal Information Controller
PIP	Personal Information Processor
PMP	Privacy Management Program
RDS	Records Disposition Schedule
S/OA	Subcontracting or Outsourcing Agreement
SIMP	Security Incident Management Policy
SPI	Sensitive Personal Information

BACKGROUND

Republic Act (RA) No. 10173 or "*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,*" otherwise known as the Data Privacy Act of 2012 (DPA), is the law that gives form to the declared policy of the State to protect the fundamental human right to privacy.

While the State recognizes the vital role of information and communications technology (ICT) in nation building, it also acknowledges its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secure and protected.

The Act serves the following purposes:

1. Protects the privacy of individuals while ensuring free flow of information to promote innovation and growth;
2. Regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data; and
3. Ensures that the Philippines complies with international standards set for data protection through the National Privacy Commission (NPC).

INTRODUCTION

NAMRIA is committed to protect the privacy, security, confidentiality, integrity, and availability of individual personal information (PI), sensitive personal information (SPI), and privileged information in compliance with the DPA, its Implementing Rules and Regulations (IRR) and other issuances of the National Privacy Commission (NPC). This manual applies to PI, SPI, and Privileged Information collected, acquired, maintained, stored, shared or disclosed by NAMRIA officials, employees, and map sales officers, including job-order workers and those hired under Individual Contract of Service as well as those outsourced through Institutional Contract of Service, and their agents.

All individuals representing NAMRIA will endeavor to safeguard personal data to which they have access to. In addition, this manual will develop and implement organizational, technical, and physical safeguards that will reasonably protect personal data from intentional and unintentional uses or disclosures that may violate DPA. Moreover, the manual will institute procedures to verify the identity of any person or entity requesting personal data and the authority of that person or entity to have access to PI, SPI, and/or Privileged Information.

This Privacy Manual outlines NAMRIA's data protection and privacy measures to guide all stakeholders in the exercise of their rights under DPA.

DEFINITION OF TERMS

For purposes of this Manual, the following terms are hereinafter defined as follows:

1. *Commission* refers to the National Privacy Commission created by virtue of RA 10173.
2. *Consent of the data subject* refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of 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.
3. *Data processing systems* refers to the structure and procedure by which personal data is collected and further processed in an information and

communications system or relevant filing system, including the purpose and intended output of the processing.

4. *Data sharing* refers to the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor;
5. *Data Sharing Agreement* refers to a contract, joint issuance or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties.
6. *Data subject* refers to an individual whose personal, sensitive personal or privileged information is processed by NAMRIA.
7. *Map sales officers* refers to other designated officers of NAMRIA Map Sales Offices from DENR and LGUs covered with Memorandum of Agreement.
8. *Personal data* refers to all types of personal information.
9. *Personal data breach* refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.
10. *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.
11. *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 (a) A person or organization who performs such functions as instructed by another person or organization; and (b) An individual who collects,

holds, processes or uses personal information in connection with the individual's personal, family or household affairs;

12. *Personal Information Processor* refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject.
13. *Privileged information* refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication;
14. *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.
15. *Security Clearance* refers to a written document signed by the Administrator issued to a specific employee that provides the authority to handle and/or access personal information.
16. *Security incident* refers to an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place;
17. *Sensitive personal information* refers to personal information:
 - a. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
 - b. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
 - c. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

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

SCOPE AND LIMITATIONS

This Privacy Manual applies to all NAMRIA officials, employees, and map sales officers, including job-order workers and those hired under Individual Contract of Service as well as those outsourced through Institutional Contract of Service, and their agents.

In this manual, personal information and personal data may be used interchangeably and will mean an individual's personal information (PI), sensitive personal information (SPI), and privileged information collectively as defined under the DPA.

PROCESSING OF PERSONAL DATA

A. Collection

NAMRIA shall only collect information which are adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

The collection of PI, SPI, and/or Privileged Information is done by lawful means and for a lawful purpose and is directly related and necessary in the fulfillment of the legal mandate and/or contractual obligations of NAMRIA with its employees, job-order workers, workers hired under institutional and individual contracts of service, service providers, clients, other government agencies, and private individuals.

Personal data collected may include information such as name, age, date of birth, gender, citizenship, address, email address, cellular/telephone numbers, government-issued identification details as well as identification cards issued by private institutions, biometrics, employment records and health records depending on the purpose for which the data are collected. These are obtained through the data subjects' filling up of official forms. These forms are essential in the provision of services to data subjects.

B. Use

When using personal data, NAMRIA employees shall make earnest efforts to limit the amount of information used or disclosed to what is only reasonably necessary in accordance with the proportionality principle.

The following standards apply to the use of PI, SPI, and/or Privileged Information:

1. NAMRIA limits access to and use of the protected personal data of individuals provided in conformity with its legal mandate and/or contractual agreements with third parties; and
2. NAMRIA officials, employees, and map sales officers, including job-order workers and those hired under Individual Contract of Service as well as those outsourced through Institutional Contract of Service and their agents, shall only have access to the amount and type of personal data necessary to carry out their duties, functions, and responsibilities and shall restrict their use, access, and disclosure of personal data to the minimum necessary;

C. Storage, Retention, and Destruction

C.1 Storage

1. NAMRIA shall ensure that documents containing personal data shall be stored appropriately to reduce the potential for incidental use or disclosure. Documents shall not be easily accessible to any unauthorized employee or visitors.
2. Paper-based records shall be maintained in a secure area that allows access by authorized employees only as needed and shall be protected from loss, damage, and destruction.
3. Records, whether in paper or digital formats, may be reviewed by authorized employees or employees having security clearance. These employees reviewing records shall do so in accordance with the minimum necessary standards.
4. Authorized employees shall review records at the designated area or workstation where the data should be located and accessed unless a different place is allowed in accordance with NAMRIA procedures.

5. Hardcopy of records shall not be left unattended in areas where employees, clients, visitors, and unauthorized individuals could easily view the records.
6. Depending on the nature of the information, NAMRIA shall implement stringent security measures in storing collected personal information and shall issue a separate and appropriate memorandum therefor.

C.2 Retention

1. NAMRIA's retention policy hinges from the principle that the longer period of retention, the more stringent security must be in place. Corollary thereto, NAMRIA shall keep PI and/or SPI no longer than what is necessary for their retention.
2. NAMRIA shall store the records until the retention period has expired based on the existing policy prescribed in the agency Records Disposition Schedule (RDS). Records shall be stored in a secure place and protected from unauthorized access and accidental/wrong destruction.
3. At the expiration of the retention period, the paper-based and electronic records shall be destroyed. Records shall be destroyed annually in accordance with the retention timeframes.
4. Records used or that may be used in a pending litigation may be exempt from scheduled destruction within a period as prescribed by the policy of NAMRIA.

In this connection, the retention period of all PI shall be based on the RDS of the agency. A copy of the RDS is hereto attached as Appendix A and made an integral part of this Manual.

C.3 Destruction of Hard Copy

1. Disposal or destruction of hard copy containing personal data shall be in accordance with Article 47, Rule 31 of the IRR of RA 9470 or the National Archives of the Philippines Act of 2007 and the attending NAMRIA RDS (Appendix A). In the absence of a policy governing the same in the RDS, the above rules shall be used as a default method.
2. NAMRIA's acceptable methods of destruction include shredding and pulverization of personal data. Records containing PI, SPI,

and/or Privileged Information shall not be thrown into an insecure trash receptacle.

3. A destruction log shall be maintained by the designated Data Protection Officer (DPO) and/or his/her assignee to identify the destroyed records. At a minimum, the destruction log shall capture the following information:
 - a. The date of destruction;
 - b. The name of the individual responsible for destroying the records;
 - c. The name of the person who witnessed the destruction; and
 - d. The method used to destroy the records.
4. Prior to the destruction of boxed items, the DPO shall verify if the retention period has expired.
5. If the records are destroyed offsite through a service provider, a Certificate of Destruction or any similar document shall be obtained attesting to destruction of the records.
6. NAMRIA shall maintain destruction documents permanently.

C.4 Destruction of Personal Data in Electronic Means

Workstations, laptops and servers use hard drives to store a wide variety of information. Personal data may be stored in a number of areas on a computer hard drive. For example, employee information may be stored in "Folders" specifically designated for storage of this type of information, in temporary storage areas, and in cache. Simply deleting the files or folders containing this information does not necessarily erase the data. The following shall serve as procedures in the destruction of personal data in electronic copy:

1. To make certain that the PI and/or SPI is totally disposed of, authorized personnel shall oversee the process and procedure in disposing the personal data.
2. If the computer is being redeployed internally or disposed of due to obsolescence, an Eraser Tool/Software shall be used to permanently delete information stored therein. After which, the hard drive may

be reformatted and a standard software image loaded on the reformatted drive.

3. If the computer is being disposed of due to damage and it is not possible to run the software program/utility to overwrite the data (i.e., Eraser Tool), then the hard drive shall be removed from the computer and physically destroyed. Alternatively, the drive can be erased by using magnetic bulk eraser. This applies to personal computer workstations, laptops, and servers.

D. Access

NAMRIA shall implement the procedures below to make certain that unauthorized physical access to its electronic information systems and the locations in which they are housed is limited, while ensuring that properly authorized access is allowed.

1. Unauthorized employees, subcontractors, and agents who access personal data, or areas where they may be accessed without being properly authorized pursuant to this procedure, shall be subject to administrative sanctions based on existing Civil Service rules.
2. The Administrative Division Chief, in consultation with the DPO, shall implement procedures to control and validate individuals' access to facilities and/or locations on a need-to-know basis.
3. The Administrator shall issue a security clearance upon the recommendation of the DPO. Coordination with other government agencies, where necessary and appropriate, shall be made in respect thereto.
4. The security clearance of employees shall be reviewed regularly and modified in accordance with NAMRIA procedures and related issuances.

E. Disclosure and Sharing

NAMRIA shall limit its uses and disclosures of personal data only to the extent allowed or required by the DPA, its IRR, and other issuances of the NPC. Unless expressly allowed or required by law, NAMRIA shall not disclose personal data to a third party without the written consent of the data subject.

In cases where personal data will be shared with the third party for a legal and authorized purpose or where the processing thereof shall be contracted to a third party, a Data Sharing Agreement and/or a

Subcontracting or Outsourcing Agreement shall forthwith be executed prior to sharing or outsourcing.

The following are permitted uses and disclosures of personal information under this manual:

1. When the disclosure to the individual is a requirement in a judicial proceeding;
2. When disclosure is required by law; and
3. When the use or disclosure is to carry out treatment, payment or health care operations, or other medical interventions;

SECURITY MEASURES

NAMRIA shall implement reasonable and appropriate physical, technical, and organizational measures for the protection of personal data. These security measures aim to maintain the availability, integrity, and confidentiality of personal data as well as to protect them against natural dangers (e.g., accidental loss or destruction) and human dangers (e.g., unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination).

A. Organizational Security Measures

1. Conduct of Privacy Impact Assessment (PIA)

NAMRIA shall conduct a Privacy Impact Assessment (PIA) relative to all activities, new projects, and systems involving the processing of personal data.

2. Designation of DPO and COP

A DPO or Compliance Officer for Privacy (COP) shall be designated through a Special Order (SO) issued by the Administrator. In the absence thereof, the Administrator shall be the default DPO. An SO may also be issued to create a Data Privacy Committee (DPC) headed by the DPO to better administer and facilitate the duties and responsibilities of the latter and the general obligations of NAMRIA in protecting personal information holdings in all its offices and facilities.

3. Functions of the DPO and/or any Other Responsible Personnel with Similar Functions

A DPO or COP of NAMRIA is hereby declared to be independent in the performance of his or her functions and is given a certain degree of autonomy by the Administrator to do the functions in protecting personal information for NAMRIA.

The designated DPO shall perform, among other things, the following, to wit:

1. Monitor the compliance of NAMRIA with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies. For this purpose, he or she may:
 - a. Collect information to identify the processing operations, activities, measures, projects, programs or systems of NAMRIA and maintain a record thereof;
 - b. Analyze and check the compliance of processing activities, including the issuance of security clearances and compliance by third-party service providers;
 - c. Inform, advise, and issue recommendations to the Administrator;
 - d. Ascertain the renewal of accreditation necessary to maintain the required standards in personal data processing and;
 - e. Advise the Administrator as regards the necessity of executing a data sharing agreement or an outsourcing contract with third parties and ensure their compliance with the law.
2. Ensure the conduct of PIA relative to activities, measures, projects, programs, or systems of NAMRIA;
3. Advise the Administrator regarding complaints and/or the exercise by the data subject of their rights (e.g., request for information, clarifications, rectification or deletion of personal data);
4. Ensure proper data breach and security incident management, including the preparation and submission of reports to NPC and other documentation concerning incidents or data breaches within the prescribed period;
5. Inform and cultivate awareness on privacy and data protection within the entire agency, including all relevant laws, rules, and regulations and issuances of NPC;

6. Advocate for the development, review and/or revision of policies, guidelines project and/or programs of NAMRIA relating to privacy and data protection by adopting a privacy by design approach;
7. Cooperate, coordinate and seek the advice of NPC and other authorities in all matters concerning data privacy and security; and
8. Perform other duties and tasks that may be assigned by the Administrator which further the interest of data privacy and security and uphold the rights of data subjects.

Except for items (1) to (3), a COP shall perform all functions of a DPO. Where appropriate, he or she shall also assist the DPO in the performance of the latter's functions.

4. Duty of Confidentiality

All employees authorized to access and/or process personal data shall be required to sign a Confidentiality or Non-Disclosure Agreement (Annex B). They shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure. Confidential documents must be labelled or marked and must be covered in the appropriate cover sheet (Annex C). This duty of confidentiality shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

5. Review of Privacy Manual

This Privacy Manual shall be reviewed and evaluated yearly or as often as necessary whenever a new process will be adopted. Privacy and security policies and practices within NAMRIA shall be updated to remain consistent with current data privacy best practices.

B. Physical Security Measures

1. Facility Security Plan

Each facility, office and/or branch, and data centers shall:

- a) Exercise care when installing any hardware or equipment to ensure that the installation is made pursuant to appropriate codes and manufacturer's instructions and to avoid damage to power supply, communication cabling, or otherwise;
- b) Change locks, access codes or other devices or applications permitting access to and within the facility as necessary and appropriate; and

- c) Ensure any and all buildings and platforms where personal data are stored, regardless of format, are sufficiently secure.

2. Workstation Security

Each workstation where personal data can be accessed or where they are processed shall be accessible only to the employee/s assigned to them. Visitors shall not be allowed to use a workstation which permits access to personal information.

3. Format of Data

Personal data in the custody of the agency may be in digital/electronic format and paper-based/physical format depending on the needs and objectives for their collection and processing.

4. Storage Type and Location

All personal data of employees, service providers, and clients in paper-based documents and 201 files shall be stored in a locked filing cabinet located at the NAMRIA. Digital/electronic files shall be stored in computers protected by passwords and antivirus and can be access only by authorized personnel.

5. Procedure in Case of Access by Inadvertence

Only authorized employees with security clearance may have access to personal information. In the event that an employee comes into contact with personal data by inadvertence or by whatever cause without authorization or under circumstances outside of his or her assigned responsibilities, the employee shall not use or disclose the information, but shall make effort to immediately contact his or her supervisor or, if not available, the designated DPO or COP for the purpose of turning over to the latter all copies of the information obtained in whatever form.

6. General Safeguards and File Maintenance

Except as otherwise provided under this Manual, employees must adhere to the following guidelines with regard to the filing and handling of PI, SPI, and/or Privileged Information:

- a) Paper Documents. When working with files containing personal data, employees must take steps to minimize access by others to that information by keeping their work areas, including desks, office space or other areas, wherever they may be, free of personal information or closing or covering files when they are not actively working with the information.

- b) **Electronic Documents.** Files containing personal data, if any, shall be in the appropriate folder with restricted access. In general, and except as specifically permitted by the DPO, personal data may not be saved on any personal computers or personal portable or other data storage devices including, without limitation, desktops, laptops, email servers, smartphones, tablets, copiers, flash drives, and external drives.
- c) **Incidental Disclosures.** Employees must ensure to prevent disclosure of personal information to unauthorized employees, clients, service providers, and other third parties. Employees must use reasonable efforts to reduce the likelihood that those communications will be overheard or viewed by unauthorized individuals.
- d) **Recording Communications.** Except in public gatherings and in meetings requiring full documentation and with sufficient notice to the attendees, no employee may use a recording device in performing their duties for the agency. In case of doubt as to whether recording is justified or not, an employee must seek the advice of the DPO.
- e) **Facsimiles and Print Jobs.** As much as possible, the use of facsimiles must not be employed whenever personal data is included in the transmission. If it cannot be prevented, an employee who transmits a facsimile must take reasonable steps to verify that the intended recipient is a person to whom he or she is required, permitted, or authorized to disclose the personal data under this Manual. All incoming facsimiles and print jobs containing PI, SPI, and Privileged Information shall be cleared from the fax machine or printer as soon as possible to avoid it being viewed by an unauthorized person.

7. Monitoring and Limitation of Access

All authorized personnel who have been given temporary access to stored personal data must fill out and register access details in a logbook. They shall indicate the date, time, duration and purpose of each access.

8. Modes of Transfer of Personal Data

Transfer of personal data in hard copy shall be through direct contact of employees concerned, courier specifically authorized by NAMRIA, and Philippine registered mail.

Transfer of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal data to third parties.

C. Technical Security Measures

1. Access Controls

All documents containing PI, SPI, and/or Privileged Information shall be kept in a location with access limited to those employees who need access to such documentation during the regular course of their duties. All passwords to access NAMRIA's ICT systems shall be kept in a location and/or format as may be determined by GISMB.

2. Integrity

In order to ensure the integrity of personal data, the DPO, through the GISMB, shall:

- a) Test, maintain, and update all software and hardware applications prior to installation and as appropriate, to ensure no damage to the agency's information and communication systems;
- b) Implement up-to-date firewalls, system security agent software, malware, patches, and virus definitions that are designed to maintain the integrity of the personal data on the agency's ICT systems connected to Internet. As appropriate, the Agency's Information and Communication Systems shall be designed to receive current security updates on a regular basis.
- c) Keep a backup of all personal data on a secure onsite storage and as much as practicable, on cloud. In case the personal information is stored on cloud through a service provider, the agency may require the service provider to be compliant with ISO/IEC 27018:2014 (Information Technology Security Techniques: Code of Practice for Protection of Personally Identifiable Information [PII] in Public Clouds Acting as PII Processors), putting in mind the recommendation of NPC and the Department of Information and Communications Technology.

3. Encryption

NAMRIA shall employ different types of encryption methods in order to protect personal information from being easily accessible. In connection thereto, measures shall be employed such as Secure Sockets Layer on the agency's website.

BREACH AND SECURITY INCIDENTS

A. Procedure for Breach Notification

Employees, contract of service workers, subcontractors or service providers who believe that unauthorized access, use or disclosure of personal data have occurred shall immediately and simultaneously report the circumstances of the suspected breach to their supervisor and/or the DPO (or, in the absence of the DPO, reports may be made to the COP). The suspected breach shall be reported within 24 hours from becoming aware thereof. The DPO shall, within 72 hours after receipt of the incident report and after securing clearance from the Administrator, report such breach to NPC in case the breach falls under those required by law to be reported thereto.

The breach report of the DPO shall include the following information, to the extent available:

1. Nature of the Breach

- a. Description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
- b. Chronology of the events leading up to the loss of control over the personal data;
- c. Approximate number of data subjects or records involved;
- d. Description or nature of the personal data breach;
- e. Description of the likely consequences of the personal data breach; and
- f. Name and contact details of the DPO or any other accountable persons.

2. Personal Data Possibly Involved

- a. Description of sensitive personal information involved; and

- b. Description of other information involved that may be used to enable identity fraud.

3. Measures Taken to Address the Breach

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

NAMRIA maintains an open-door policy regarding compliance with NPC Circular No. 2016-03 (Personal Data Breach Management). Employees are encouraged to speak with the DPO, COP or other appropriate individual regarding any concerns they may have with NAMRIA compliance program or initiatives designed to maintain and enhance privacy and security controls.

Periodic breach drill shall be provided so that employees will understand their responsibilities in relation to Personal Data Breach Management policies and procedures. Training opportunities may occur during staff meetings, through emails, via online training or informally posting important updates on the office bulletin board and Imail.

Failure to report a suspected breach to the supervisor and/or DPO or COP may result in a disciplinary action against the employee.

B. Creation of a Data Breach Response Team

NAMRIA shall create a Data Privacy Committee to be headed by the DPO. The duly established DPC shall be performing the function of the Data Breach Response Team (DBRT). As such, the team shall be responsible for ensuring immediate action in the event of a security incident or personal breach.

The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall for ensure immediate action to be taken in the event of a security incident or personal data breach. Likewise, it shall execute measures to mitigate the adverse effects of the incident or breach.

C. Measures to Prevent and Minimize the Occurrence of Breach and Security Incidents

NAMRIA shall regularly conduct a PIA to identify risks, threats, and vulnerabilities in the data processing system. Personnel directly involved in the processing of personal data shall be required to attend trainings and seminars for capacity building. A periodic review of policies and procedures being implemented in the agency shall be undertaken.

D. Procedure for Recovery and Restoration of Personal Data

NAMRIA shall always maintain a backup file for all personal data under its custody. In the event of security incident and/or personal data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

E. Documentation and Reporting Procedure of Security Incidents or Personal Data Breach

As part of NAMRIA's annual report, the DBRT shall prepare the documentation pertaining to all security incidents or personal data breaches that have occurred in the agency within a period of one (1) year and shall submit the same to NPC before the set deadline.

The report shall contain the following:

1. Description of the nature of the incident or breach;
2. Personal data possibly involved;
3. Measures undertaken by the team to address the breach and reduce the harm or its negative consequences; and
4. Agency details.

RIGHTS, INQUIRIES, AND COMPLAINTS OF DATA SUBJECTS

In order to uphold the rights of the data subject under DPA, the following policies and procedures are adopted:

A. Inquiries and Complaints

NAMRIA respects the right of a data subject to information as well as recognizes his or her right to file a complaint. In order to uphold these rights of the data subject, the following policies and procedures are available to the data subject:

1. Inquiries

Data subjects may inquire or request for information from the DPO regarding any matter relating to the processing of their personal data under the custody of NAMRIA, including the data privacy policies implemented to ensure the protection of their personal data. Inquiries shall be made in writing and sent personally or via email at dpo@namria.gov.ph. Responses to inquiries shall be given within 15 working days from the receipt of the request.

2. Complaints

Any complaints for violation of data privacy rights or any breach of personal data in the possession or under the custody of NAMRIA shall be addressed to the DPO and shall be made in writing. The complaint shall also be filed through dpo@namria.gov.ph.

Upon the receipt of the complaint, the DPO shall, within a reasonable period of time, conduct a verification of the allegations in the complaint, and if warranted, conduct an official investigation in cases of serious security breach as provided under applicable laws and rules.

Within 15 working days from the receipt of the complaint, the DPO shall send a letter to the complainant apprising him or her of the actions being taken on the complaint and on what stage of investigation the complaint has gone through to resolve the issue.

After verification and investigation, the DPO shall submit his or her recommendation to the Administrator for approval.

During the entire process, the DPO shall document the following:

- a. Proceedings;
- b. Outcome of the complaint/s; and
- c. Complete logs of complaint/s by entering the resolution and any required follow-up actions.

The DPO shall maintain documentation of complaints received and their disposition for a period as prescribed by NPC. In the absence of such prescription, the maintenance and retention of the said documentation shall be in accordance with the NAMRIA RDS.

Employees and agents may not intimidate, threaten, coerce, discriminate against or take any other retaliatory action against the person served, clients or any other person filing a complaint. Violations of this policy shall be dealt with severely in accordance with Civil Service Laws.

As much as possible, the DPO shall try to settle the controversy within the organization and use all available modes of dispute resolution.

B. Right to Correct

An individual who believes the PI and/or SPI in his/her record is incorrect or incomplete may request an amendment or correction to the information following the procedures below:

1. If there is a data subject request, the employee responsible for accessing the record must assist the latter in completing the request for amendment using the Client Request Form (CRF). (Refer to Appendix D)
2. The employee responsible for accessing the record must act on the request for amendment within a reasonable time after receipt of the request.
3. If there is a need to extend the process of approving and acting on the request, the employee responsible for accessing the record shall give the person requesting written notice for such, stating the reason for the extension.
4. If the request for amendment or correction is granted, the employee responsible for accessing the record must document the fact of correction or amendment indicating the change and the date when it was effected. He or she shall then affix his or her signature thereto. The CRF must be attached to the amended entry. The person requesting shall be informed that the amendment has been approved and effected. There must be a similar method of documentation in changing personal data in the computer system.
5. Copies of the amendment/correction must be provided to other units of the agency which may have interest in the amended information.

6. The request must be denied if the PI and/or SPI was not recorded by the NAMRIA unit where request is being sought or is inaccurate or incomplete and/or is not supported by competent evidence.
7. If the responsible employee accessing the record denies the request for amendment, he/she must provide the requester an explanation for the denial within a reasonable period.
8. A person requesting for correction or amendment can request for the reconsideration of a denied request.
9. If a request for amendment is sent directly to the DPO, he or she shall work directly with the NAMRIA unit concerned to evaluate and resolve the request.
10. Knowledge of a violation or potential violation of this policy must be reported directly to the DPO.

C. Right to Access and/or Obtain Copy

The following are the procedures in the exercise of a data subject's rights to access and obtain copy of his/her personal data.

1. Any request to access and/or obtain a copy of his or her own personal data being stored or processed by NAMRIA shall use the CRF.
2. Upon receipt of a request, the personnel with appropriate authority shall act on the request by either:
 - a. Informing the individual of approval of the request; or
 - b. Sending a letter of denial particularly stating the reason therefor.
3. If there is a need to extend the process of approving and acting on the request, the employee responsible for processing the request shall give the requester a written notice for such, stating the reason for the extension.
4. Personnel with security clearance must be the one who should process this kind of request using proper access and authorization procedures.
5. If the request pertains to information stored and maintained electronically in one or more designated record sets and if the data subject's request is for an electronic copy of such information, the

employee responsible shall provide the requesting data subject with access to the PI and/or SPI in electronic form and format, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the DPO and the person requesting.

6. The request and grant of access or furnishing of copy of the PI and/or SPI to the data subject shall be documented.
7. If a request for access or to obtain a copy is sent directly to the DPO, he or she shall work directly with the NAMRIA unit concerned to evaluate and resolve the request.
8. Knowledge of a violation or potential violation of this policy must be reported directly to the DPO.

D. Right to be Informed

The NAMRIA Privacy Notice shall comply with DPA, its IRR, and other issuances of NPC. Specifically:

1. The privacy notice informs the person applying for or receiving services of:
 - a. The reason for collection, uses, and disclosures of PI and/or SPI that may be made by NAMRIA;
 - b. The rights of a data subject with respect to his/her personal data; and
 - c. NAMRIA's duties in safeguarding such PI, SPI, and Privileged Information.
2. The privacy notice shall be written in plain language and shall be made available in languages understood by a substantial number of clients served by NAMRIA, using industry parlance. NAMRIA shall endeavor to make a Filipino translation of the notice.
3. NAMRIA employees shall provide or disclose the Privacy Notice to the data subject prior to the processing of personal data.
4. At the time the Privacy Notice is provided, NAMRIA employees shall make a good faith effort to obtain the consent of the client requesting products and services.

5. The DPO shall post a copy of the Privacy Notice in the area or location most prominent to the eyes of the viewing public such as the entrance lobby at NAMRIA's various offices and facilities. The same shall also be posted on NAMRIA's official website and disseminated over the intranet system for employees.
6. Whenever the Privacy Notice is revised, the DPO shall make the revised privacy notice available upon request on or after the effectivity date of the revision.
7. The revised Privacy Notice shall be subjected to the same posting and information dissemination procedure as mentioned above.
8. Any individual or employee who has knowledge of a violation or potential violation of this Procedure shall report it directly to the DPO for proper action.

MISCELLANEOUS PROVISION

In view of DAO 97-24 entitled "DENR Policy on the Release or Disclosure of Information," the use, access, and disclosure of personal data shall be conducted consistent with the provisions of DPA and this manual.

SEPARABILITY CLAUSE

If any portion or provision of this Privacy Manual is declared null and void, the other provisions not affected thereby shall continue to be in force and effect.

EFFECTIVITY

The provisions of this Privacy Manual are effective this ____ day of _____ 2018 and shall be officially observed, until revoked or amended.

APPENDICES

APPENDIX A

{Insert NAMRIA Records Disposition Schedule}

APPENDIX B

{Insert Confidentiality Agreement}

APPENDIX C

{Insert Confidential Cover Sheet}

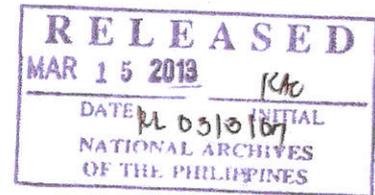
APPENDIX D

{Insert Client Request Form}



NATIONAL ARCHIVES OF THE PHILIPPINES
Pambansang Sinupan ng Pilipinas

March 13, 2013



DR. PETER N. TIANGCO, CESO I
Administrator
National Mapping & Resource Information Authority
Fort Bonifacio, Taguig City

Attention: **MS. LINDA SD PAPA**
Deputy Administrator/Chairperson, RMIC

Sir:

We are returning a copy of your Records Disposition Schedule which was approved on March 12, 2013.

Please reproduce and disseminate to all action units for their guidance in the disposition of records. Kindly acknowledge receipt hereof.

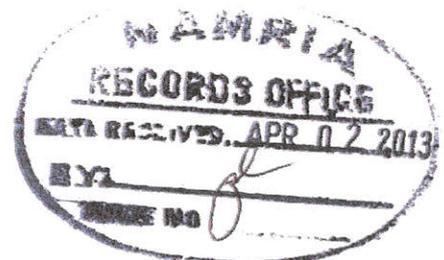
Thank you for your interest in bringing about an effective, efficient, and economical records management program.

Very truly yours,

VICTORINO MAPA MANALO
Executive Director

By:


VIRGINIA E. DARLUCIO
Deputy Executive Director
3113





NATIONAL ARCHIVES OF THE PHILIPPINES
Pambansang Sinupan ng Pilipinas

RELEASED
MAR 15 2013
DATE: *RL 6313107*
NATIONAL ARCHIVES
OF THE PHILIPPINES

March 13, 2013

DR. PETER N. TIANGCO, CESO I
Administrator
National Mapping & Resource Information Authority
Fort Bonifacio, Taguig City

Attention: **MS. LINDA SD PAPA**
Deputy Administrator/Chairperson, RMIC

Sir:

We are returning a copy of your Records Disposition Schedule which was approved on March 12, 2013.

Please reproduce and disseminate to all action units for their guidance in the disposition of records. Kindly acknowledge receipt hereof.

Thank you for your interest in bringing about an effective, efficient, and economical records management program.

Very truly yours,

VICTORINO MAPA MANALO
Executive Director

By:

[Signature]
VIRGINIA E. DARLUCIO
Deputy Executive Director *3/13*

RECEIVED BY:
Cherrylin D. Mendoza
Cherrylin D. Mendoza

NATIONAL ARCHIVES OF THE PHILIPPINES
Pambansang Sinupan ng Pilipinas
RECORDS DISPOSITION SCHEDULE

1. AGENCY NAME:

NATIONAL MAPPING AND RESOURCE
INFORMATION AUTHORITY

2. ADDRESS:

Lawton Ave., Fort A. Bonifacio, Taguig City

3. SCHEDULE NO.

4. DATE PREPARED:

July 19, 2012

5. ITEM NUMBER	6. RECORD SERIES TITLE AND DESCRIPTION	7. RETENTION PERIOD			8. REMARKS
		Active	Storage	Total	
1	OFFICE OF THE ADMINISTRATOR, DEPUTY ADMINISTRATORS AND HEAD EXECUTIVE ASSISTANT DIRECTIVES/ISSUANCES Issued by/or the head of the agency documenting policies/functions/programs of the agency		PERMANENT		
2	LEGAL CASES Administrative Civil	7 years		7 years	Decisions are PERMANENT
3	MEMORANDA OF AGREEMENT (MOA) / OF UNDERSTANDING (MOU) Active Geodetic Network, Map Sales Offices, Tide Stations and other facilities Technical Assistance and Special Projects	5 years	5 years	10 years	PERMANENT if implemented
4	BOARD RESOLUTIONS		PERMANENT		
5	SUBPOENA	3 years		3 years	or To be filed with appropriate case
	STAFF SUPPORT SERVICES ADMINISTRATIVE DIVISION				
6	APPROVED RATIONALIZATION PLAN		PERMANENT		
7	APPROVED TREASURY BONDS OF SPECIAL DISBURSING OFFICERS (SDOs)	1 year	5 years	6 years	
8	COMMITTEE FILES ON PERSONNEL ACTION Decorum and Investigations on Anti-Sexual Harassment Gender and Development Grievance Magna Carta Performance Management Personnel Development Personnel Selection Board Program on Awards and Incentives for Service Excellence	5 years	5 years	10 years	
		3 years	3 years	6 years	
		3 years	3 years	6 years	
		3 years	3 years	6 years	
		3 years	3 years	6 years	
		3 years	3 years	6 years	
		3 years	3 years	6 years	
		1 year		1 year	
9	COMMUNICATIONS / CORRESPONDENCES Non-routine Routine				To be filed with appropriate record series
		2 years		2 years	
10	CONTRACTS Personnel Services Procurement or Outsourcing of Goods and Services	5 years		5 years	
		5 years	5 years	10 years	
11	CUSTOMER ORDER SLIPS	1 year		1 year	

RELEASED
MAR 12 2013
DATE: 03/12/13 INITIAL: KAC
NATIONAL ARCHIVES OF THE PHILIPPINES

IMPORTANT: Pursuant to Section 18, Article III, RA 9470 s. 2007, "No government department, bureau, agency and instrumentality shall dispose of, destroy or authorize the disposal or destruction of any public records, which are in the custody or under its control except with the prior written authority of the executive director."

5. ITEM NUMBER	6. RECORDS SERIES TITLE AND DESCRIPTION	7. RETENTION PERIOD			8. REMARKS
		Active	Storage	Total	
12	FREE ISSUANCE ON REQUESTS OF CHARTS AND MAPS	2 years		2 years	After acted upon
13	INCOMING/OUTGOING CORRESPONDENCES LOGBOOKS	2 years		2 years	After date of last entry
14	MAP STOCK INVENTORIES	1 year		1 year	
15	ORGANIZATIONAL CHARTS		PERMANENT		
16	QUALITY MANAGEMENT SYSTEM (QMS) Core Procedure (3) Manual Procedure (5) Standard Operating Instruction (21)		PERMANENT		
17	RECORDS MANAGEMENT IMPROVEMENT COMMITTEE (RMIC) RECORDS	3 years	3 years	6 years	After updated
18	SALES REPORTS	1 year		1 year	
	<u>MEDICAL/DENTAL CLINIC</u>				
19	EMPLOYEES' DENTAL AND MEDICAL RECORDS	2 years	3 years	5 years	
20	DENTAL AND MEDICAL REPORTS Dental and Medical Cases Inventory of Medicine and Supplies	2 years 1 year	3 years	5 years 1 year	
21	STOCK CARDS Medicines Medical Supplies	1 year		1 year	
	<u>PERSONNEL SECTION</u>				
22	APPLICATIONS Applicants Leave of Absence and Supporting Documents Retirement/Resignation	3 years 1 year 1 year		3 years 1 year 1 year	After recorded in the leave cards
23	ATTENDANCE MONITORING SHEETS	1 year		1 year	
24	AUTHORITIES/REQUESTS TO CREATE OR FILL VACANT POSITIONS	2 years		2 years	After position had been filled-up
25	DAILY TIME RECORDS	1 year		1 year	After data had been leave cards and post-
26	LOCAL AND FOREIGN TRAINING PROGRAMS	3 years		3 years	After superseded.
27	MEMBERSHIP FILES Government Service Insurance System Home Development Mutual Fund PhilHealth	5 years	10 years	15 years	After separated.
28	MERIT PROMOTION PLANS	1 year		1 year	
29	PERFORMANCE FILES Appraisal Summary of Performance Rating	1 year 5 years		1 year 5 years	
30	PERSONNEL ACTION REPORTS Civil Service Commission Report on Personnel Action/Report on Appointment Issues Civil Service Commission Report on Separation Department of Environment and Natural Resources Manpower Strength Report	2 years		2 years	

RELEASED
MAR 12 2018 KAC
DATE PLO31885 INITIAL
NATIONAL ARCHIVES
PHILIPPINES

5. ITEM NUMBER	6. RECORDS SERIES TITLE AND DESCRIPTION	7. RETENTION PERIOD			8. REMARKS
		Active	Storage	Total	
31	PERSONNEL FOLDERS (201 FILE)	5 years	10 years	15 years	After separation/retirement
32	PLANTILLA OF PERSONNEL	PERMANENT			Other copies dispose after 3 years
33	POSITION DESCRIPTION OF PERSONNEL	PERMANENT			
34	PROFILE OF RESOURCE PERSONS	2 years	3 years	5 years	
35	STATEMENT OF ASSETS, LIABILITIES AND NETWORTH	10 years		10 years	
36	TRAINING EVALUATION QUESTIONNAIRE	1 year		1 year	After data had been
37	TRAINING / WORKSHOP / SEMINAR COMPENDIUM	5 years		5 years	
<u>PROPERTY AND SUPPLY SECTION</u>					
38	ACCREDITATION OF SUPPLIES	1 year		1 year	Upon expiration
39	ACKNOWLEDGEMENT RECEIPTS OF EQUIPMENT (ARE) / MEMORANDUM RECEIPTS OF EQUIPMENT (MRE) , SEMI-EXPANDABLE AND NON-EXPANDABLE PROPERTIES	2 years		2 years	Upon clearance / separation
40	BIDS AND AWARDS COMMITTEE (BAC) FILES	5 years	5 years	10 years	After contract of winning had been
41	CANVASS/REQUESTS FOR PRICE QUOTATIONS	2 years		2 years	10 years if attached to vouchers; others after 2 years
42	CONSOLIDATED ANNUAL PROCUREMENT PLANS	3 years		3 years	
43	EQUIPMENT LEDGER CARDS	2 years		2 years	After equipment had been disposed
44	EQUIPMENT, SUPPLIES AND WASTE MATERIAL RECORD	2 years	2 years	4 years	
45	INSPECTION AND INVENTORY REPORT (Unserviceable Equipment)	1 year		1 year	
46	INVENTORY OF EQUIPMENT	1 year		1 year	After updated
47	JOB ORDERS	1 year		1 year	
48	PURCHASE ORDER LOGBOOK	4 years		4 years	
49	PURCHASE REQUESTS	1 year		1 year	
50	REQUEST ISSUANCE SLIP / SUPPLIES ISSUANCE VOUCHER (Withdrawal Slip)	1 year		1 year	
51	TURN-IN SLIP OF EQUIPMENT	2 years		2 years	
<u>FINANCIAL MANAGEMENT DIVISION</u>					
52	ADVICES OF CHECKS ISSUED/CANCELLED Accounts Payable/Retirement Gratuity General Fund 101 Pensions Trust Fund 184	4 years		4 years	

RELEASED
MAR 12 2013 *Kto*
DATE 4/03/85 INITIAL
NATIONAL ARCHIVES
OF THE PHILIPPINES

5. ITEM NUMBER	6. RECORDS SERIES TITLE AND DESCRIPTION	7. RETENTION PERIOD			8. REMARKS
		Active	Storage	Total	
68	INDICES OF PAYMENTS Employees Sundry Payment by Warrant	5 years	5 years	10 years	
		PERMANENT			
69	INTERNAL AUDIT PLANS	5 years		5 years	
70	INTERNAL AUDIT REPORTS Compliance Audit Financial Audit Retirees Pension Payroll Fund Transfer from 101 to 102 General Fund (CSORSBF)	5 years	5 years	10 years	
		PERMANENT			
71	JOURNAL ENTRY VOUCHERS	5 years	7 years	12 years	Provided post-audited, settled and not involved any case
		PERMANENT			
72	LIST OF REMITTANCES Loans Premiums				
		PERMANENT			
73	OFFICIAL CASHBOOK				
		PERMANENT			
74	SCHEDULES OF ACCOUNTS RECEIVABLES	3 years		3 years	
75	STATEMENT OF ACCOUNTS PAYABLE Annual Monthly/Quarterly				
		PERMANENT			
		5 years	5 years	10 years	
76	SUMMARIES OF UNLIQUIDATED OBLIGATIONS AND PAYABLES	5 years	5 years	10 years	
77	TRIAL BALANCES AND SUPPORTING DOCUMENTS Annual Trial Balance Accounting's Copy Monthly/Quarterly Trial Balance Cumulative Results and Operations-Unappropriated	5 years	5 years	10 years	After annual financial had been published
		2 years		2 years	After consolidated into financial report
		PERMANENT			
78	UTILITY BILLS	5 years	5 years	10 years	After settled
79	VOUCHERS AND OTHER SUPPORTING DOCUMENTS Disbursements Journals Liquidations Reimbursement Expenses Receipts	5 years	5 years	10 years	Provided post-audited, settled and not involved any case
		PERMANENT			
80	WARRANT REGISTER				
		PERMANENT			
81	WITHOLDING TAX CERTIFICATES	4 years		4 years	After superseded
	<u>PLANNING AND OPERATIONS DIVISION</u>				
82	AGENCY ACCOMPLISHMENT REPORTS Annual Accomplishment Bi-monthly/Monthly Organizational Transition Program Review and Analysis				
		PERMANENT			
		2 years		2 years	After incorporated in the annual report
		PERMANENT			
		2 years		2 years	
83	CONSOLIDATED ANNUAL WORK AND FINANCIAL PLAN	3 years		3 years	
84	MEDIUM TERM PUBLIC INVESTMENT PROGRAM/MEDIUM TERM PUBLIC EXPENDITURE PROGRAM	3 years	2 years	5 years	

RELEASED
MAR 12 2013
DATE: 03/12/2013 INITIAL: [Signature]
FILE: 1031385
NATIONAL ARCHIVES
COLLECTIONS

5. ITEM NUMBER	6. RECORDS SERIES TITLE AND DESCRIPTION	7. RETENTION PERIOD			8. REMARKS
		Active	Storage	Total	
85	MINUTES OF MEETING Board Staff		PERMANENT		
		1 year		1 year	
86	CHARTER (CREATION OF NAMRIA)		PERMANENT		
87	FORWARD BUDGET ESTIMATES	5 years	2 years	7 years	
88	NAMRIA OPERATING MANUAL		PERMANENT		
89	ANNUAL PLANNING GUIDELINES	1 year		1 year	After superseded, provided 1 copy is retained for reference
90	PROJECT FOLDER Foreign-assisted Regular Special	2 years		2 years	PERMANENT if
	<u>SECURITY AND INTELLIGENCE DIVISION</u>				
91	CLOSED CIRCUIT TELEVISION FOOTAGES	2 years		2 years	
92	EMERGENCY RESPONSE PLAN		PERMANENT		
93	INVESTIGATION REPORT	5 years	5 years	10 years	After resolved
94	LICENSE OF FIRE ARMS	2 years		2 years	
95	SCHEDULE OF DUTY	1 year		1 year	
96	SID LOGBOOKS Duty Officer and Guard Equipment Tally out Official Business Pass Visitors	2 years		2 years	After date of last entry PERMANENT for VIP
	<u>MAPPING AND GEODESY DEPARTMENT (MGD)</u>				
97	ANALOG DATA Administrative Maps (Reproducibles) Aerial Photographs (with index) Diapositives Negatives Topographic Maps (Reproducibles)		PERMANENT		
		2 years		2 years	
			PERMANENT		
			PERMANENT		
98	CERTIFICATIONS	2 years		2 years	
99	DELIVERY OF MAP STOCKS	2 years		2 years	
100	DIGITAL DATA Administrative Maps Aerial Photographs Satellite Images Topographic Maps		PERMANENT		
101	GEODETIC CONTROL SURVEY FILES Digital Field Data (Raw and processed) Gravity Horizontal Vertical		PERMANENT		
102	MAP STOCK ISSUANCES LOGBOOK	2 years		2 years	After date of last entry
103	MGD DATA SHARING AGREEMENT	2 years	3 years	5 years	
104	PHOTO/IMAGE CONTROL POINTS SURVEY RECORDS	2 years		2 years	

RELEASED
MAR 12 2013 KAE
DATE R10338C INITIAL
NATIONAL ARCHIVES
OF THE UNITED STATES

5. ITEM NUMBER	6. RECORDS SERIES TITLE AND DESCRIPTION	7. RETENTION PERIOD			8. REMARKS
		Active	Storage	Total	
105	PRINTING PLATES COLLECTION	1 year		1 year	
106	WAREHOUSE FILES Inventory Report Stock Cards	2 years		2 years	
REMOTE SENSING AND RESOURCE DATA ANALYSIS DEPARTMENT (RSRDAD)					
107	CERTIFICATION OF LAND CLASSIFICATION (LC) STATUS		PERMANENT		
108	COURT ORDER ON LC	3 years	4 years	7 years	Decisions are PERMANENT
109	FOREST COVER STATISTICS		PERMANENT		
110	LC LOGBOOKS	1 year	3 years	4 years	
111	LC STATISTICS		PERMANENT		
112	RSRDAD DATA SHARING AGREEMENT	2 years	3 years	5 years	
113	THEMATIC DATA Analog Digital		PERMANENT		
HYDROGRAPHY DEPARTMENT (HD)					
114	ANALOG NAUTICAL CHARTS		PERMANENT		
115	ATTENDANCE MONITORING REPORT (Survey Vessel)	1 year		1 year	
116	CHART HISTORY FILES Chart-Draft-Plots Master Charts Nautical Charts (Aid proof)		PERMANENT		
		3 years		3 years	After issuance of new chart
117	CHART REPRODUCIBLE MATERIALS (Positive/Negative)		PERMANENT		
118	COAST PILOT FIELD DATA		PERMANENT		
119	COMMISSIONED OFFICERS AND ENLISTED PERSONNEL FILES Assignment Orders Board Orders Efficiency and Separation Examinations Inquiry Personnel Board for Commissioned Officers and Enlisted Personnel Profile Summary Cases		PERMANENT		
120	CREW LIST	1 year		1 year	After updated
121	CERTIFICATIONS	2 years		2 years	
122	DIGITAL TIDAL DATA		PERMANENT		
123	ELECTRONIC NAVIGATIONAL CHARTS	2 years	3 years	5 years	After updated
124	HD DATA SHARING AGREEMENT	2 years	3 years	5 years	
125	HYDROGRAPHIC PUBLICATIONS		PERMANENT		Retain 2 copies for reference

RELEASED
MAR 12 2013
DATE RECORDED INITIAL
NUMBER OF COPIES
BY THE RECORDS UNIT

5. ITEM NUMBER	6. RECORDS SERIES TITLE AND DESCRIPTION	7. RETENTION PERIOD			8. REMARKS
		Active	Storage	Total	
126	INCIDENT REPORTS	2 years	3 years	5 years	
127	LIST OF STATION BILLET (Duties and responsibilities of officers and crew)	2 years		2 years	
128	MAGNETIC DATA FILES Balance Magnetometric Zero (BMZ) Data Declination Inclination Observation Description of Magnetic Stations Digital Data Field Observation Magnetic data Epoch 2010 Magnetograms Quartz Horizontal Magnetometer (QHM) Data Solar Maps Standardization Elements		PERMANENT		
129	MANUAL ON COMMISSIONED OFFICERS AND ENLISTED PERSONNEL		PERMANENT		
130	OCEANOGRAPHIC SURVEY REPORTS Annual Inspection and Releveling Reconnaissance Retrieval Tidal leveling Tide House Damage Establishment Maintenance		PERMANENT		
		2 years	3 years	5 years	
		2 years	3 years	5 years	
			PERMANENT		
		2 years	3 years	5 years	
131	PERSONNEL INFORMATION OF ON-THE-JOB-TRAINING (OJT), SEAMAN APPRENTICE AND CONSULTANTS	2 years		2 years	
132	PHYSICAL OCEANOGRAPHIC OBSERVATION FILES Tides Analogue data Conductivity Digital Data Salinity and Densities Surface Temperature		PERMANENT		
133	RESOLVED DELINEATION OF MUNICIPAL WATER RECORDS		PERMANENT		
134	SHIP REPORTS Damaged Drydocking Ship's Status		PERMANENT		
135	SURVEY REPORTS Descriptive Reports Hydrographic Surveys Topographic Surveys Smooth Sheets Hydrographic Topographic		PERMANENT		
136	SURVEY VESSEL LOGBOOK Rough Smooth Bridge Engine Liberty Book	2 years		2 years	After date of last entry
		10 years	10 years	20 years	
		5 years	5 years	10 years	
		2 years		2 years	
137	TIDE AND CURRENT TABLES		PERMANENT		

RELEASED
MAR 12 2013
DATE 11/02/13
NATIONAL ARCHIVES
1117 COLLEGE BLVD
COLLEGE PARK, MD 20740

5. ITEM NUMBER	6. RECORDS SERIES TITLE AND DESCRIPTION	7. RETENTION PERIOD			8. REMARKS
		Active	Storage	Total	
138	UNIT ASSIGNMENTS	1 year		1 year	
139	VESSEL REPORTS	PERMANENT			After consolidated in the annual report
	Accident	2 years	2 years	4 years	
	Hull Board	2 years	2 years	4 years	
	Maintenance	2 years		2 years	
	Monthly				
	Petroleum Oil Lubricant (POL) Consumption	1 year		1 year	
	Schedule of Watches	1 year		1 year	
	Technical Inspection/Damage	2 years	3 years	5 years	
INFORMATION MANAGEMENT DEPARTMENT (IMD)					
140	CATALOGUE OF NAMRIA PRODUCTS AND SERVICES	2 years	2 years	4 years	After updated
141	CERTIFICATION OF ACCREDITATION OF GEOMATICS TRAINING CENTER (GTC)	2 years	2 years	4 years	After renewal
142	CLIENT PERCEPTION ANALYSIS REPORTS	2 years		2 years	
143	DOCUMENTATION OF NAMRIA HISTORICAL EVENTS	PERMANENT			
144	GTC PARTICIPANTS DIRECTORY/PROFILE	2 years	2 years	4 years	
145	GTC TRAINING MANUALS	5 years	5 years	10 years	
146	IMD DATA SHARING AGREEMENTS	2 years	3 years	5 years	
147	INFORMATION SYSTEMS STRATEGIC PLANS	3 years	2 years	5 years	After revision
148	MANUALS ON GEOGRAPHIC INFORMATION SYSTEMS STANDARDS	PERMANENT			
149	NEWS CLIPPINGS	2 years	3 years	5 years	Digital Files PERMANENT
150	PRESS RELEASES	PERMANENT			
151	PUBLICATIONS (Record Set)	PERMANENT			
152	SYSTEMS DEVELOPMENT FILES	2 years	3 years	5 years	Digital Files PERMANENT
ENGINEERING SERVICES DEPARTMENT (ESD)					
153	BUILDING, GROUND AND PERIMETER LOT PLANS	PERMANENT			
154	CERTIFICATE OF VEHICLE REGISTRATION (CR)	1 year		1 year	After vehicle had been disposed
155	LOCAL NETWORK DESIGN	PERMANENT			
156	MAINTENANCE LOGBOOKS	2 years		2 years	After date of last entry
	Computer Facilities				
	Repair and Maintenance of Technical and Communication Equipment				
	Vehicle				
157	MATERIAL/EQUIPMENT LEDGER OF VEHICLES (Spare parts)	2 years		2 years	After certified or declared non-operational of vehicle

RELEASED
MAR 12 2013
DATE: MAR 12 2013 INITIAL: R/E
KLO338C
NATIONAL ARCHIVES
OF THE BUREAU OF LAND MANAGEMENT

5. ITEM NUMBER	6. RECORDS SERIES TITLE AND DESCRIPTION	7. RETENTION PERIOD			8. REMARKS
		Active	Storage	Total	
158	MONTHLY REPORTS Fuel/Petroleum Oil Lubricant (POL) Consumption Status of Vehicle	1 year		1 year	
159	TRIP TICKETS	1 year		1 year	
160	VEHICLE LAND REGISTRATION OFFICE (LTO) REGISTRATION/CERTIFICATE OF COVERAGE/ VEHICLE OFFICIAL RECEIPT	1 year		1 year	After renewal

RELEASED

MAR 12 2013 *KTB*

DATE: MAR 12 2013 INITIAL: *KTB*

NAME: KL03138C OFFICE: [unclear]

OFFICER: [unclear] [unclear]

9. Prepared by:

Fedman
FEBRINA E. DAMASO

OIC, Assistant Director
Chairperson, NAMRIA Archival Committee

Concepcion A. Bringas
CONCEPCION A. BRINGAS

OIC, Information Services Division
Vice Chairperson, NAMRIA Archival Committee

11. Recommending Approval:

Linda Sd Papa
LINDA SD PAPA

Deputy Administrator
Chairperson, NAMRIA Records Management and Improvement Committee

10. Assisted by:

Janet A. Francia
JANET A. FRANCIA

Senior Records Management Analyst

Ehxia R. Dondonilla
EHXIA R. DONDONILLA

Records Management Analyst I

12. Approved:

Dr. Peter N. Tiangco, Cesol
DR. PETER N. TIANGCO, CESO I

Administrator, NAMRIA

TO BE ACCOMPLISHED BY THE NATIONAL ARCHIVES OF THE PHILIPPINES

This Records Disposition Schedule

- is being returned for improvement / correction
- is being recommended for approval

Jennie C. Litigio
JENNIE C. LITIGIO

Chairman
Records Management Evaluation Committee

*all 3.4.13
gin 3/4/13*

3/8/13

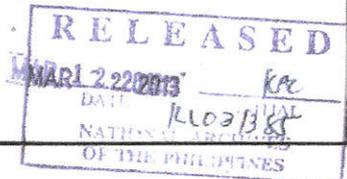
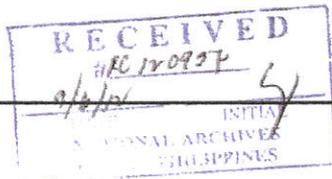
Date

APPROVED:

Victorino Mapa Manalo
VICTORINO MAPA MANALO

Executive Director

Date



CONFIDENTIAL

THIS IS A COVER SHEET
(Unclassified if not covering Confidential Document)

WARNING

THE UNAUTHORIZED DISCLOSURE OF INFORMATION CONTAINED IN ATTACHED DOCUMENT(S) WHILE NOT ENDANGERING NATIONAL SECURITY WILL BE PREJUDICIAL TO THE INTEREST OR PRESTIGE OF THE NATION, ANY GOVERNMENTAL ACTIVITY, OR WILL 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 AND 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



Republic of the Philippines
Department of Environment and Natural Resources
NATIONAL MAPPING AND RESOURCE INFORMATION AUTHORITY
Lawton Ave., Fort Bonifacio, Taguig City 1634

DATE:

SECURITY CLEARANCE CERTIFICATE

THIS IS TO CERTIFY that the following NAMRIA personal information processors have been granted **INTERIM SECURITY CLEARANCE**, under the provisions of Executive Order Number (No.) 608 dated 30 March 2007, Memorandum Circular (MC) No. 78 dated 14 August 1964 as amended by MC No. 176 dated 18 July 1968, and the Data Privacy Act of 2012, to handle, gain access, and review **restricted** and **confidential** matters and information:

THIS CERTIFICATE is valid for six (6) months only, unless sooner revoked or withdrawn.

Usec. PETER N. TIANGCO, PhD
Administrator

Distribution:

- Copy 1: Security Office-AO
- Copy 2: 201 File
- Copy 3: Data Protection Officer



NAMRIA OFFICES:

Main : Lawton Avenue, Fort Bonifacio, 1634 Taguig City, Philippines Tel. No.: (632) 810-4831 to 41
Branch : 421 Barraca St. San Nicolas, 1010 Manila, Philippines, Tel. No. (632) 241-3494 to 98

www.namria.gov.ph