



Republic of the Philippines  
**OFFICE OF THE SECRETARY**  
Elliptical Road, Diliman 1100 Quezon City  
+63(2) 8928-8741 to 64 and +63(2) 8273-2474

## **DEPARTMENT ORDER**

NO. 15

Series of 2024

**SUBJECT : PRIVACY MANUAL OF THE DEPARTMENT OF AGRICULTURE**

---

### **I. BACKGROUND**

Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (“DPA”), aims to protect personal data in government and private sector information systems.

It mandates that all organizations processing personal data shall establish policies and implement measures to ensure data safety and security, thus upholding individual privacy rights. Personal information controllers and processors must take reasonable steps to protect personal data from natural and human dangers, such as accidental loss, unlawful access, and fraudulent misuse.

Each organization must create a Privacy Manual to inform its personnel about the risks involved and measures to be taken in case of potential breach. This Privacy Manual provides guidance for compliance with the DPA, its Implementing Rules and Regulations (“IRR”), and National Privacy Commission (“NPC”) issuances, detailing protocols for data protection throughout its lifecycle from collection to destruction, to ensure the rights of data subjects are met.

### **II. INTRODUCTION**

The Department of Agriculture (“DA” or this “Department”) processes a wide range of information, including personal data from stakeholders/shareholders, employees, and other relevant parties. The DA is committed to ensuring that in doing so, data privacy rights are respected and upheld.

Thus, this Department hereby adopts this Privacy Manual in strict compliance with the DPA, its IRR, and other applicable privacy issuances of the NPC. This Privacy Manual serves as a comprehensive guide for all officials, staff, and personnel, outlining the standards and procedures to ensure that the collection, storage, processing, sharing, and disposal of personal data adhere to the principles set forth in the DPA and its IRR. By following these guidelines, this Department aims to uphold the highest standards of data privacy and protection, safeguarding the rights and interests of all individuals whose data it processes and protects.

### **III. SCOPE AND LIMITATIONS**

This Privacy Manual governs the processing of personal data by this Department and its personal information processors. All offices, employees, staff, and personnel of this Department, regardless of the nature of their employment, must strictly comply with the terms outlined in this Privacy Manual. For purposes of this Privacy Manual, all bureaus, agencies, and corporations are understood to be excluded from its coverage.

Should this Privacy Manual lack specific data privacy policies or provisions, the DPA, its IRR, and privacy issuances of the NPC shall be applied.

#### IV. DEFINITION OF TERMS

- A. **Consent** refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal data. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so.
- B. **Data Protection Officer (DPO)** refers to an individual designated by the Secretary of this Department to ensure its compliance with the DPA, its IRR, and other privacy issuances of the NPC: *Provided that*, the designated DPO must meet the qualifications established by applicable law and relevant privacy issuances of the NPC.
- C. **Data Processing Agreement (DPrA)** refers to an agreement or any similar document that binds the personal information processor to this Department as PIC, which sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations of the personal information processor, and the geographic location of the processing under the DPrA.
- D. **Data Sharing** refers to the sharing, disclosure, or transfer to a third party of personal data under the custody of a personal information controller.<sup>1</sup> For purposes of this Privacy Manual, it is understood that there are two kinds of data sharing: internal and external.

**Internal Data Sharing** refers to the disclosure, sharing, transfer, or exchange of personal data within the confines of the Department proper.

**External Data Sharing**, in contrast, refers to the disclosure, sharing, transfer, or exchange of personal data to parties outside the Department proper. Disclosure, sharing, transfer, or exchange of personal data to attached bureaus, agencies, and corporations, partners, clients, suppliers, and other governmental bodies are classified as external data sharing.

External Data Sharing to or from this Department shall be covered by a Data Sharing Agreement.

---

<sup>1</sup> National Privacy Commission, Data Sharing Agreements (NPC Circular No. 2020-03)

- E. Data Sharing Agreement (DSA)** refers to a contract, joint issuance or any similar document which sets out the obligations, responsibilities and liabilities of the PICs involved in the transfer of personal data between or among them, including the implementation of adequate standards for data privacy and security and upholding the rights of the data subjects.
- F. Data Subject** refers to an individual whose personal data is processed by this Department.
- G. Personal Data** refers to all types of personal information, sensitive and non-sensitive included.
- H. Personal Data Breach** refers to a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of or unauthorized processing of personal data. It compromises the availability, integrity, or confidentiality of personal data.
- I. 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.
- J. Personal Information Controller (PIC)** 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.
- K. Personal Information Processor (PIP)** refers to any natural or juridical person qualified to act as such under the DPA to whom this Department, as a PIC, has outsourced the processing of personal data pertaining to a data subject. All outsourcing of any form of processing of personal data shall be covered by a Data Processing Agreement.
- L. 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.
- M. Retention Period** refers to the specific period of time established and approved by the National Archives of the Philippines as the life span of records, after which they are deemed ready for permanent destruction.

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

**O. 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 person, 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 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.

**P. Valueless Records** refer to all records that have reached the prescribed retention periods and outlived the usefulness to the agency or the government as a whole.

## V. PROCESSING OF PERSONAL DATA

### A. Data Privacy Principles

This Department processes personal data in accordance with applicable laws and ensures that all such processing are reasonable and appropriate. This Department is committed to process data in a manner that upholds the following principles:

- a) **Transparency** - The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
- b) **Legitimate purpose** - The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.
- c) **Proportionality** - The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

### B. Collection

This Department collects personal and sensitive personal information from its personnel, beneficiaries, stakeholders, and other third parties. Each office has its own methods for data collection, whether manual or automated, in compliance with the criteria for data processing required by the DPA<sup>2</sup>. Generally, the types of personal data collected by this Department include, but are not limited to the following:

- a) Basic personal information such as the name, date of birth, gender, marital status, and citizenship, including supporting documents such as government-issued ID details
- b) Contact details such as the home address, mobile number, and email address
- c) Specimen signatures
- d) Education, employment, and business details
- e) Religious and farmer or fisherfolk affiliations
- f) Images via CCTV and other similar recording devices which may be observed when visiting our offices and/or using our other facilities
- g) Account transactions, movements and interactions with third parties such as merchants

### **C. Use**

Personal data shall be processed solely for the specified and legitimate purposes, as communicated to the data subject, and only with their consent or as allowed by the DPA<sup>3</sup>, its IRR and other issuances. The processing of personal data will serve the following purposes, among others:

- a) To generate updated data necessary in identifying beneficiaries for agriculture and fishery programs of the government;
- b) To conduct a more comprehensive stakeholder analysis and needs prioritization;
- c) To enhance and advance the development of this Department's workforce;
- d) To facilitate this Department's intervention programs by registering beneficiaries;
- e) To monitor this Department's distribution of goods and assistance;
- f) To respond to court orders, instructions and requests from authorities including regulatory, governmental, and law enforcement;
- g) To discharge our mandate pursuant to Philippines laws and international agreements which the Philippines has ratified;
- h) To respond to, process and handle your queries, requests, feedback, suggestions and complaints;
- i) To conduct studies and researches for the purpose of reviewing, developing and improving our provision of product and services in accordance with our mandate; and
- j) To prevent, detect, investigate crime and manage the safety and security of our premises and services (including but not limited to conducting security clearances and carrying out CCTV surveillance).

---

<sup>2</sup> Sec. 13. Sensitive Personal Information and Privileged Information. Data Privacy Act of 2012.

<sup>3</sup> Section 12 of Data Privacy Act of 2012.

## D. Storage, Retention and Destruction

All offices and units shall ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. The Administrative Service and the Information and Communications Technology Service (ICTS) shall implement appropriate security measures and protocols in storing collected personal data, depending on the nature of the information.

This Department is equally committed to implementing stringent data **retention policies** that comply with legal requirements and align with best practices. Personal data under the DA's custody shall not be retained longer than necessary.

In accordance with the National Archives of the Philippines (NAP) General Circular No. 9, dated 20 January 2009, records will be retained only as per the approved schedule<sup>4</sup> outlined in the NPC Circular. This approach ensures that the data is managed responsibly, balancing operational needs with the obligation to protect individual privacy.

Upon the expiration of the retention period, personal data will be securely disposed of as follows:

### 1. Paper Format

Personal data in paper format, along with any attachments, will be retained for **five (5) years** from the time they are encoded into the system and/or digitized. After this period, the paper forms and attachments will be disposed of and destroyed by shredding.

### 2. Digital/Electronic Data

Digital or electronic data will be retained for **five (5) years** from the time they are classified as valueless records or are no longer necessary. After this retention period, all digital records and their copies will be permanently deleted from the database and all storage devices.

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

It is understood that these retention periods shall not apply if:

- a. There is any other law or regulation that requires the retention of such data for a longer period; or

---

<sup>4</sup> See Annex A.  
Page 6 of 19



- b. The retention of personal data is still necessary for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has not been terminated.

#### **E. Access**

Access shall be granted only to authorized personnel as described above. Access shall be granted solely for lawful purposes and shall not be used for any activity contrary to law, morals, public policy, public order, and good customs.

#### **F. Disclosure and Sharing**

This Department, together with its officials, employees, staff, and personnel, regardless of the nature of their employment, shall exercise due diligence and the highest level of care when processing personal data.

Unauthorized disclosure of any personal data by any official, employee, staff, personnel, or agent, absent the necessary approvals or agreements and without the consent of the data subject shall constitute as a violation of this Manual and shall be dealt with in accordance with applicable laws and rules.

##### **a) Perpetuity of Confidentiality**

All confidential information that comes to the knowledge and possession of an official, employee, or agent shall subsist even after the severance of their employment contract/service.

##### **b) Internal Data Sharing**

Any disclosure, sharing, transfer, or exchange of personal data between offices/units within this Department shall be covered by an official request letter submitted to the DA office/unit that has custody of the personal data requested, indicating the following:

- i. The data sets that is being requested;
- ii. The purpose of the request;
- iii. The duration of retention; and
- iv. An undertaking not to disclose, give access to, transmit, or share to any office other than the requesting office, or persons outside the requesting office, the requested data sets.

The DA office/unit that has custody of personal data must maintain a record of all requests, together with the above-enumerated information found on the request letter.

This process ensures that personal data is securely transmitted through official channels and is shared for valid and authorized purposes only.

### **c) External Data Sharing**

Disclosure, sharing, or transfer of personal data with external entities is permitted only when covered by a DSA and when the relevant data subjects have given their consent.

## **VI. SECURITY MEASURES**

Data security is the practice of safeguarding digital information against unauthorized access, corruption, destruction, modification, theft, or disclosure. This Department is committed to ensuring that the data of its stakeholders remains secure and confidential. To achieve this, the DA will establish and enforce robust physical, technical, and organizational measures designed to uphold privacy and protect sensitive information.

### **A. Organizational Security Measures**

#### **1. Data Protection Officer**

Pursuant to Section 10 of the NPC Circular No. 2022-04, a designation and registration of DPO in any government agency is mandatory. The appointment of a DPO enhances customer service and strengthens the DA's ability to respond effectively to the increasing public demand for robust data protection measures. Below are his/her functions as DPO:

- a) Monitor the PIC's or PIP's compliance with the DPA, its IRR, NPC issuances, and other applicable laws and policies. For this purpose, he/she may:
  - i. Collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
  - ii. Analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service provider;
  - iii. Inform, advise, and issue recommendations to the PIC or PIP;
  - iv. Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
  - v. Advise the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;
- b) Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;
- c) Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
- d) Ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of



- reports and other documentation concerning security incidents or data breaches within the prescribed period;
- e) Inform and cultivate awareness on privacy and data protection within the DA, including all relevant laws, rules and regulations and issuances of the NPC;
  - f) Cultivate awareness on privacy and data protection within the DA, including all relevant laws, rules and regulations and issuances of the NPC;
  - g) Advocate for the development, review and/or revision of policies, guidelines projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;
  - h) Serve as the contact person of the PIC or PIP *vis-a-vis* data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;
  - i) Cooperate, coordinate, and seek advice of the NPC regarding matters concerning data privacy and security;
  - j) Supervise DPOs and Compliance Officers for Privacy who shall hereafter be designated for each unit and/or office, to whom the DPO may delegate some of the functions herein enumerated; and
  - k) Perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

## **2. Compliance Officers for Privacy (COPs)**

Aside from having a DPO, this Department shall designate a COP for each of its sub-unit/office. The COPs shall be under the supervision of the DPO, in accordance with relevant privacy issuances of the NPC.

Each Regional Field Office of the DA shall have a COP to assist the DPO in overseeing data privacy compliance within their jurisdiction. Below are the functions of COPs:

- a) Assist the DPO in the performance of her functions;
- b) Monitor their RFO's or data processing system's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies and submit monthly reports to the DPO;
- c) Review documents in connection with data privacy, such as Data Sharing Agreements, in accordance with the DPA, its IRR, and NPC issuances;
- d) Upon the instructions of the DPO, collect information to identify the processing operations, activities, measures, projects, programs, or systems of their respective RFOs or data processing systems, and maintain a record thereof;
- e) Analyze and check the compliance of processing activities;
- f) Conduct a preliminary assessment of the propriety of issuing security clearances to and compliance by third- party service providers, and provide recommendations to the DPO;
- g) Assist the DPO in issuing data protection advice and recommendations to the PIC or PIP;

- h) Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing;
- i) Confer with and assist the DPO in ascertaining the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the DPA, its IRR, and NPC issuances;
- j) Ensure proper data breach and security incident management by the PIC or PIP, including the latter' s preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
- k) Inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC;
- l) Advocate for the development, review and/ or revision of policies, guidelines, projects and/ or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;
- m) Serve as the representative of the DPO and the secondary contact person of the PIC or PIP with respect to the RFO or the data processing system *vis-à-vis* data subjects, the NPC, and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;
- n) Assist the DPO in cooperating, coordinating, and seeking the advice of the NPC regarding matters concerning data privacy and security;
- o) Perform other duties and tasks that may be delegated by the DPO in furtherance of data privacy compliance and security and to uphold the rights of the data subjects; and
- p) Submit quarterly reports to the DPO detailing his/ her performance of the above-enumerated duties and responsibilities.

### **3. Data Breach Response Team (DBRT)**

A Data Breach Response Team shall be responsible for promptly addressing any security or data breaches within the DA. During a data breach, the team shall immediately assess the extent of the incident and notify the DPO. The team shall conduct an initial assessment of the incident or breach which involves the determination of the scope and severity of the breach and ensure that appropriate actions are taken to mitigate risks.

The Data Breach Response Team<sup>5</sup> shall be composed of:

- a. Director, ICTS;
- b. Regional Executive Directors (RED) of the Regional Field Offices (RFO) of the DA;
- c. Chief, Network Operations and Management Division (NOMD), ICTS; and
- d. Head, Information Communication Technology Unit (ICTU).

Pursuant to Section 5 of NPC Circular 16-03<sup>6</sup>, entitled "*Personal Data Breach Management*", the Head of the DBRT is authorized to make immediate decisions

---

<sup>5</sup> See Annex C.

<sup>6</sup> See Annex D.

on critical actions when necessary. In addition to supporting the secure management of information and data assets, the DBRT is responsible for mitigating the impact of any data breach within this Department.

The DBRT shall perform the following functions:

**a. *Preparation and Planning***

- i. Develop within thirty (30) days from the date of this issuance a security incident management policy and response plan that details and outlines the steps to be taken if a data breach occurs.
- ii. Conduct risk assessments through identification of potential vulnerabilities and risks to the DA's data and systems.
- iii. Assist in establishing communication protocols that defines how the DBPT will communicate with this Committee and the PIC internally and externally during a breach.

**b. *Monitoring, Detection, and Assessment***

- i. Continuously monitor systems and networks for vulnerabilities and potential security threats.
- ii. Recognize when a data breach is in progress or has occurred.
- iii. Determine the scope and nature of the breach and its potential impact.

**c. *Containment and Mitigation***

Take immediate action to isolate compromised systems or networks to prevent further damage.

**d. *Recovery and Remediation***

- i. Bring affected systems back online and ensure that they are secure.
- ii. Recover and restore lost or compromised data.
- iii. Strengthen security measures to prevent future breaches.

**e. *Documentation and Reporting***

Keep detailed records of all actions taken during the incident response process and submit report to the DPO.

**f. *Training and Awareness***

Assist in providing training to the employees to raise awareness about data security and how to respond to potential breaches.

**4. Data Privacy Committee**

This Department shall always have a Data Privacy Committee that is tasked to oversee and ensure the effective implementation and compliance of data privacy policies and practices within the organization. Headed by the DPO of the DA, it serves as a governance body to manage data protection efforts systematically.

The Data Privacy Committee shall be composed of the following:

- a. DPO
- b. COPs
- c. DBRT
- d. Secretariat

## **5. Trainings and Seminars**

This Department shall ensure that relevant officials, employees, and personnel attend trainings and seminars at least once a year, in order to understand their respective duties and responsibilities with respect to processing of personal data and to keep abreast with ever-evolving privacy rules and regulations. These officials and employees shall help in fostering a culture of awareness and compliance within the DA.

The trainings and seminars will ensure that both new hires and existing staff are equipped to discharge their functions by undergoing proper and informative training.

## **6. Privacy Impact Assessments**

A Privacy Impact Assessment (PIA)<sup>7</sup> is a tool used to evaluate the potential privacy risks associated with processes, information systems, programs, software modules, devices, or other initiatives that handle personal information. Through consultation with stakeholders, the PIA identifies privacy risks and guides the implementation of necessary measures to mitigate those risks effectively.

This Department shall conduct a PIA at least once every two (2) years, or as often as the law or pertinent rules require, covering all activities, projects, and systems that involve the handling of personal data. Each office/unit of the DA directly responsible for data processing must likewise conduct a PIA at least once every two (2) years.

## **7. Executing Non-Disclosure Agreements**

Non-Disclosure Agreements (NDAs) are legal contracts that protect sensitive and/or confidential information from being disclosed to unauthorized third parties.

This Department recognizes the necessity of executing NDAs in maintaining the confidentiality and integrity of personal and organizational data. By binding parties to confidentiality obligations ensures that data remains secure and is neither disclosed nor misused.

The DA shall execute NDAs, apart from other applicable agreements, before any disclosure, sharing, transfer, or exchange of organizational data to/with third parties takes place.

Moreover, all employees, staff, and personnel, regardless of the nature of their employment, shall be asked to sign an NDA. All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

## **8. Review of the Data Privacy Manual**

This Department, through the Data Privacy Committee, shall conduct annual reviews of this Privacy Manual to ensure that the its data protection policies and procedures stay up-to-date, effective, and compliant with changing laws, technologies, and organizational needs. It is understood that such annual review will begin in 2026, unless a need for an earlier review arises.

## **B. Physical Security Measures**

### **1. Format of Personal Data**

Personal Data processed by this Department are either in digital format or physical format.

### **2. Storage Type and Location**

- a) **Data in Physical Form:** It shall be kept in locked filing cabinets located at a secure designated storage area. Spot check shall be done twice a week and a report therefor shall be prepared. Access to it shall only be permitted by authorized personnel.
- b) **Data in Digital Form:** It shall be securely managed and stored by the data-collecting office and the ICTS only in password-protected DA-issued computers and devices. Should external storage or third-party digital storage solutions be necessary, it shall be password protected. All personal data managed and stored by the ICTS shall be stored in their acquired Cloud Service with sufficient security protocols.

### **3. Access Procedure of Agency Personnel**

Access to personal data stored in physical form is strictly limited to authorized personnel of the office responsible for the personal data. For digital data, access is

restricted to authorized personnel from the data-collecting office and designated ICTS staff.

Access by other personnel may only be granted with the express approval of the Director or an officer of equivalent or higher rank within the office with custody of the personal data.

#### **4. Monitoring and Limitation of Access to Room or Facility**

Authorized personnel responsible for data custody will conduct bi-weekly spot checks to ensure that physical data prevents from unlawful destruction, alteration and contamination. A report shall be prepared by the said authorized personnel.

The Director or any officer of equivalent rank or higher of the custodial office will designate not more than two (2) authorized personnel per division or office to manage the key that grants access to this data.

Data stored in the ICTS servers is protected by password access and restricted to authorized personnel only. In addition, a biometric lock system has been implemented for enhanced security. The ICTS personnel are required to have backups of the stored data on their cloud infrastructure to ensure data integrity and availability.

#### **5. Design of Office Space/Work Station**

Storage areas and secured file cabinets must be located in a secure area within the office, safeguarded against natural disasters, unauthorized external access, and similar threats. Computers and other devices used for data processing shall be positioned to prevent public visibility, ensuring the privacy of sensitive information.

Biometric lock systems and passwords are implemented to secure data stored on ICTS servers and in the cloud. Authorized personnel must ensure that these locks and passwords are regularly updated and changed to maintain security.

#### **6. Persons Involved in Processing, and their Duty and Responsibilities**

Confidentiality must be upheld and strictly maintained throughout every stage of data processing. Authorized personnel are prohibited from unlawfully giving access to sharing or using any information or data they have accessed or acquired thereto.

Protocols and standard procedures in accessing or entering the data storage room may be established by the PIC or PIP.

#### **7. Modes of Transfer of Personal Data within the Organization**

To secure handling of personal data within this Department, stringent measures are in place for data transfer both internally and externally. The NDAs, DSAs, DPrAs, and request letters are key instruments used to safeguard these processes.

Data transfers should conducted via electronic mail must be done using an official DA-issued email or by uploading files to a server through the secure file transfer protocol (SFTP) provided by the ICTS.

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

## **8. Retention and Disposal Procedure**

- A. Retention policies stated in Section V(D) shall be strictly observed at all times. The authorized personnel must monitor the retention period of personal data and identify which ones are due for disposal or destruction.
  
- B. Personal data shall be securely disposed of or discarded to prevent unauthorized processing, unauthorized access, or unauthorized disclosure to third parties or the public, and to avert any harm to the data subjects. To secure disposal of personal data, the following measures shall be implemented based on the format of records:
  - a) Any personal data contained in physical or paper format shall be disposed of through shredding. This method ensures that the documents are irreversibly destroyed, preventing any possibility of reconstruction or unauthorized access.
  
  - b) Personal data stored digitally or electronically must be permanently deleted from all databases, storage devices, and backups. This process should include the use of secure data deletion methods that prevent data recovery, such as overwriting the data multiple times or using specialized data wiping software.

Additionally, when decommissioning or repurposing storage devices, the ICTS and all custodial offices must ensure that all personal data has been securely erased or that the device itself has been physically destroyed to prevent any potential data breaches.

## **C. Technical Security Measures**

### **1. Monitoring for security breaches**

The ICTS has implemented a Next-Generation Firewall (NGFW) to enhance perimeter security and monitor potential breaches. This system provides real-time notifications for any security alerts, ensuring prompt response to threats.

In addition, ICTS has deployed Darktrace, an advanced AI-driven cybersecurity solution designed to protect data within our cloud infrastructure. Darktrace offers a comprehensive dashboard that provides network visibility, allowing for the swift identification of compromised devices, users, or servers.

The ICTS shall conduct a quarterly inspection of all devices and databases containing personal data. It shall ensure that all such devices are equipped with cybersecurity solutions capable to combat personal data compromises, security incidents, and personal data breaches.

## 2. Security features of the software/s and application/s used

- a) **Endpoint Protection Solutions:** These are security measures installed on devices like computers and smartphones to protect against threats like malware and unauthorized access.
- b) **Secure Sockets Layer (SSL):** SSL is a protocol that encrypts data sent between a user's browser and a website, ensuring that sensitive information remains private and secure.
- c) **Web Application Firewall (WAF):** A WAF is a security tool that monitors and filters incoming traffic to web applications, protecting them from attacks such as SQL injection and cross-site scripting.
- d) **Intelligent Threat Service in the Cloud:** This refers to cloud-based security services that use advanced analytics to detect and respond to potential threats in real time, safeguarding data stored in the cloud.

## 3. Process for regularly testing, assessment and evaluation of effectiveness of security measures

Most data processing systems of this Department have undergone Vulnerability Assessment & Penetration Testing (VAPT) done by the Department of Information and Communications Technology-Computer Emergency Response Team (DICT-CERT).

VAPT is a security testing service identifying security vulnerabilities in an application, network, endpoint, and cloud that can be obtained in an unauthorized access or potential harm. The primary objective is to provide organizations with actionable recommendations for enhancing their security posture and reducing the risk of cyber-attacks.

The ICTS shall identify data processing systems that are yet to undergo VAPT and shall facilitate the immediate conduct of the same. The ICTS shall likewise prepare prioritization schedule, identifying when each of the data processing systems of this Department must undergo periodic VAPT.



#### **4. Encryption, authentication process, and other technical security measures that control and limit access to personal data**

The ICTS has implemented advanced security measures, including Multi-Factor Authentication (MFA) and One-Time Pin (OTP), across most of its systems. These measures are designed to enhance the confidentiality and security of sensitive data. By requiring multiple forms of verification, MFA and OTP provide an additional layer of protection, significantly reducing the risk of unauthorized access and ensuring that the DA's data remains secure.

### **VII. BREACH AND SECURITY INCIDENTS**

#### **A. Measures to prevent and minimize occurrence of breach and security incidents**

The ICTS has deployed a Next-Generation Firewall (NGFW) with an Internet Access Policy to ensure robust data security and confidentiality. This policy consists of carefully crafted rules and configurations in the program designed to manage, filter, and secure the organization's network traffic as it interfaces with the internet through the NGFW.

Next-Generation Firewalls significantly enhance traditional firewall capabilities by incorporating advanced features such as deep packet inspection, intrusion prevention systems (IPS), application awareness and control, and user identity management. These capabilities empower the ICTS to enforce stringent security protocols, safeguard sensitive information, and maintain the integrity of the organization's data infrastructure.

Moreover, the Anti-Virus software has been installed to add an additional layer of security for the protection of this Department's data from potential threats.

The ICTS is hereby mandated to keep abreast with the latest developments and recommend the most appropriate solutions and tools that will strengthen the cybersecurity and privacy measures of this Department.

#### **B. Procedure for Recovery and Restoration of Personal Data**

The ICTS shall ensure that all databases are securely backed up through manual processes. In addition to these manual backups, Virtual Machines (VMs) or Server Clones are created as a safeguard.

A Virtual Machine is a software-based computer system that emulates the operations of a separate physical computer, allowing for the replication and preservation of its functionality and data.

#### **C. Notification Protocol**

The Head of the DBRT shall notify the DPO, relevant COP(s), the Data Privacy Committee within twenty-four (24) hours and the NPC within seventy-two (72) hours from becoming aware of or reasonably believing that a personal data breach has occurred.

If the breach is likely to pose a real risk to the rights and freedoms of the affected data subjects, the Head of the DBRT must also notify the affected individuals within the same seventy-two (72) hour period. This notification must be done in a manner that enables the data subjects to take appropriate precautions or other measures to protect themselves from potential consequences.

#### **D. Documentation and Reporting Procedure for Security Incidents and/or Personal Data Breach**

The personnel who first become aware of a security incident or personal data breach must complete a Data Security Incident Report<sup>8</sup>. This report should be submitted promptly to their immediate supervisor, the DBRT, and the DPO.

The DBRT is responsible for preparing a comprehensive report documenting each incident or breach. Additionally, they must compile an **annual report** containing all incidents, both of which are to be submitted to the Secretary, through the Data Privacy Committee, and NPC within the required timeframe.

### **VIII. INQUIRIES AND COMPLAINTS**

This Department fully acknowledges and upholds the rights of data subjects, particularly emphasizing the following:

- a) Right to reasonable access to his or her personal data being processed by the personal information controller or personal information processor;
- b) Right to dispute the inaccuracy or error in the personal data;
- c) Right to request the suspension, withdrawal, blocking, removal, or destruction of personal data; and
- d) Right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of personal data.

Inquiries or complaints related to personal data collected by the DA, including concerns about this Department's data privacy and security policies, can be addressed by contacting this Department's DPO at [dpo@da.gov.ph](mailto:dpo@da.gov.ph).

If any inquiry or concern relates to a particular RFO or custodial office (i.e., RSBSA, FFEDES, etc.), then any such inquiry or concern may be lodged before the COP of the relevant DA office/unit. The said COP shall address the inquiry or concern and report the same, together with the response given, to the DPO.

### **IX. SEPARABILITY CLAUSE**

---

<sup>8</sup> See Annex E.

If any clause, sentence, or provision of this Department Order shall be declared unconstitutional, the other provisions not affected thereby shall remain valid and subsisting.

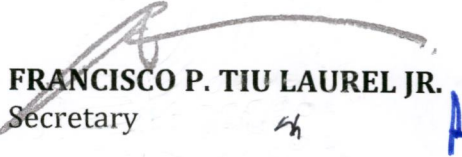
**X. REPEALING CLAUSE**

All other previous orders, issuances, rules and regulations inconsistent with or contrary to this Department Order are hereby repealed and revoked.

**XI. EFFECTIVITY**

The provisions of this Data Privacy Manual shall be effective immediately upon approval and shall remain in effect until revoked in writing.

Done this 16<sup>th</sup> day of September 2024.

  
**FRANCISCO P. TIU LAUREL JR.**  
Secretary



DA-CO-OSEC-DO20240930-00012