MEMORANDUM ORDER NO. 2024-002

RE : THE CITY GOVERNMENT OF SAN FERNANDO, PAMPANGA'S PRIVACY MANUAL

PRIVACY MANUAL

I. BACKGROUND

Republic Act (R.A.) No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect personal data in information and communications systems both in the government and the private sector.

It ensures that entities or organizations processing personal data establish policies and implement measures and procedures that guarantee the safety and security of personal data under their control and custody, thereby upholding an individual's data privacy rights. A personal information controller or personal information processor is instructed to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

To inform its personnel of such measures, the City Government of San Fernando, Pampanga (CGSFP) hereby creates this Privacy Manual. This Privacy Manual serves as a guide or handbook to ensure the City Government of San Fernando, Pampanga's compliance with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the National Privacy Commission (NPC).

This Privacy Manual shall provide for the standard procedure of the CGSFP on the access, collection, use, and processing of any and all Personal Data handled by the CGSFP in the normal course of its operations, mandates, and functions provided for under RA No. 7160, otherwise known as the "Local Government Code of 1991," and other relevant laws. It also encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances, directed toward the fulfillment and realization of the rights of data subjects.

This Privacy Manual is designed to be a living document. It may be revised to address emerging operational needs, policy development, including systems update, upgrade, or improvement. Moreover, the policies, measures, and procedures embodied in this Privacy Manual shall be constantly and regularly reviewed and updated in accordance with the programs, project, activities, and the agenda of the City of San Fernando, Pampanga (CSFP).

II. INTRODUCTION

This Privacy Manual is hereby adopted in compliance with DPA, its IRR, and other relevant laws, rules and regulations and policies, including issuances of the NPC and other relevant government agencies. The LGU respects and values the data privacy rights of all Data Subjects, and makes sure that all personal data collected from its clients, customers, and the general public are processed

in adherence to the general principles of transparency, legitimate purpose, and proportionality under the DPA.

This Privacy Manual shall inform the Data Subjects of our data protection and security measures, and may serve as guide in exercising one's rights under the DPA.

This Privacy Policy shall be posted in conspicuous areas, and shall be accessible to the public, through the LGU's website, bulletin boards, and/or a written document upon request—for purposes of informing the public and the Data Subjects about the types of personal information that will be collected, the sources of Personal Data, the purpose of processing, the methods of collection, including the use of cookies, trackers, and automated processors, and the Data Subjects' rights, among others.

III. DEFINITION OF TERMS

a. *Act or DPA* – refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012;

b. *Compliance Officer for Privacy (COP)* – refers to an individual or individuals who, under the supervision of the DPO, monitor internal compliance and ensure that the CGSFP is in compliance with data protection laws;

c. *Consent of the Data Subject* - refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of 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;

d. *Data Breach* – refers to unauthorized access, disclosure, use, alteration, destruction, damage, loss or processing of data compromising the security, confidentiality, integrity or availability of data or information under the custody of the LGU;

e. *Data Privacy Compliance Committee (DPCC)* – a committee created by the CGSFP that will ensure compliance with Republic Act No. 10173, its IRR, the issuances of the NPC, and all other relevant laws and issuances. The DPCC shall evaluate, suggest and recommend to the City Mayor, propose courses of action, act, and if within its authority, decide on matters relating to data privacy, which shall ensure not only compliance with the privacy laws, but also the development of sustainable privacy policies, systems, and operations in the local government unit;

f. *Data Protection Officer or DPO* – refers to an individual designated by the head of agency to be accountable for the agency's compliance with the DPA, its IRR, and all applicable laws and regulations for the protection of data privacy and ensuring confidentiality of information and information security;

g. *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: Provided, that only personal information controllers shall be made parties to a data sharing agreement;

h. *Data Subject* — refers to an individual whose personal, sensitive personal or privileged information is processed by the LGU. It may refer to public officials (whether elected or

appointed), their staff, personnel of the LGU (whether permanent, casual, job order or contractual), its constituents, customers and clients;

i. *Head of Agency* – refers to the Local Chief Executive of the City of San Fernando, Pampanga (CSFP);

j. *Local Government Unit (LGU)* – refers to the City of San Fernando, Pampanga. The LGU shall act as the PIC, but subject to any applicable Data Sharing and/or Outsourcing Agreement entered into by the LGU;

k. *National Privacy Commission (NPC)* – refers to the government agency created under the DPA, which is tasked to administer and implement the provisions of the DPA, and to monitor and ensure compliance of the country with international standards set for data protection;

l. *Personal Data* – shall refer to personal, sensitive personal, and privileged information, collectively. Personal Data may include, but shall not be limited to, an individual's name, or a person's postal or electronic mail address, telephone number, social security number, date of birth, mother's maiden name, official state or country-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, government aid account number, bank account number, personal identification number, unique biometric data such as fingerprint, voice print, retina or iris image or other unique physical representation, unique identification number, address or routing code, medical records, telecommunication identifying information or access device or other information that, by itself or when combined with other information accessible to the person accessing it, can be used to identify a person or access a person's financial or personal resources. A payment card number and any accompanying code assigned to the card to permit its use also constitutes Personal Data;

m. *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;

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

o. *Personal Information Processor (PIP)* – refers to any natural or juridical person qualified to act as such under the DPA to whom a personal information controller may outsource the processing of personal data pertaining to a data subject. The LGU representative or personnel shall serve as the PIC;

p. *Privacy Impact Assessment (PIA)* – refers to the process undertaken and used by a government agency or a private entity to identify, evaluate, and manage privacy risks and impacts in relation to existing or prospective projects, ventures, initiatives, systems, processes or any act by the government agency or private entity;

q. *Privileged Information* – refers to any and all forms of data, which under the Rules of Court and other pertinent laws constitute as privileged communication;

r. *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;

s. *Security Breach or 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 shall include, but not limited to, incidents that would result to a personal data breach, if not for the safeguards that have been put in place;

t. *Sensitive Personal Information* – refers to personal information:
   (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliation;
   (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
   (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
   (4) Specifically established by an executive order or an act of Congress to be kept classified; and

u. *Third Party* – refers to any natural or juridical person, public authority, agency or any other entity other than the Data Subject, the Controller and person who, under the direct authority of the Controller, are authorized to process Personal Data.

IV. SCOPE AND LIMITATIONS

All public officials (whether elected or appointed), their staff, and all personnel of the LGU (whether permanent, casual, job order or contractual) shall comply with the terms set out in this Privacy Manual.

This Privacy Manual shall govern the collection, access, use, and processing of any and all Personal Data handled by all officials, staff, personnel, and employees of the LGU, regardless of the contractual arrangement or employment of such individual, pursuant to his/her Office or Department's mandate and functions, including all individuals, organizations or entities contracting, dealing or transacting with the LGU.

V. PROCESSING OF PERSONAL DATA

A. Collection

The LGU shall collect only Personal Data that are necessary to avail the services, programs, activities, and benefits offered by the LGU, based on a lawful criteria for processing. Methods of collecting Personal Data may be done through forms, whether electronic or manual, duly accomplished by the concerned Data Subject/s, in accordance to all relevant rules of laws relating to the collection of Personal Data.

When transacting with the LGU, we collect information such as, but not limited to, the following, to wit:

1. Personal information (i.e., Name Address, Gender, Civil Status, Birthdate, Birthplace, Citizenship, Age, etc.);
2. Contact Information (i.e., Email Address, Phone Number, Telephone Number, and other relevant information in connection with the transactions with the City Government of San Fernando, Pampanga);
3. Data about your personal circumstances, such as family background, history, marital status, government records, and other relevant circumstances and employment records; and
4. Any or all information obtained through interviews, and/or other forms of personal data collection.

The LGU shall collect personal information and/or sensitive personal information depending on the service/s, program/s, activity/ies, and/or benefit/s availed by the Data Subject, which in all cases be only to the extent that is necessary for specific and legitimate purposes, based on a lawful criteria for processing.

All service/s, program/s, activity/ies, and/or benefit/s involving data gathering and collection of personal information and/or sensitive information shall be initially conferred with the Data Privacy Compliance Committee (DPCC) in the crafting of PIA relative to the data processing system/s/manual/tool/s used for the purpose.

The LGU and the DPO shall exercise reasonable efforts to confirm that when Personal Data are collected from persons other than the Data Subject, those third-party sources have collected the Personal Data fairly and lawfully.

B. Use

The Personal Data collected may be used only for the purposes for which they were collected, in relation to the service/s, program/s, activity/ies, and/or benefit/s availed by the Data Subject, as well as for purposes of documentation, processing of applications and contracts, and general administrative use.

Aside from the foregoing, Personal Data may likewise be processed for the mandated reports by the Department of the Interior and Local Government (DILG) and other relevant government agencies, annual reportorial requirements of the LGU, the necessary reports and postings in the LGU's bulletin boards and official website, and other necessary and mandatory reportorial and publications of the LGU for the transparency of government transactions.

If the Personal Data that was previously collected is to be used for purposes not previously identified, the LGU, prior to using the Personal Data for the new purpose, shall:

a. Notify the Data Subject, and document the new purpose;
b. Obtain and document the consent or withdrawal of consent to use the Personal Data for the new purpose; and
c. Ensure that Personal Data is being used in accordance only with the purposes consented to by the Data Subject or, if consent was withdrawn, not used.

In any case, the preceding paragraph shall not apply where the processing is based on a lawful criteria, in cases where the rights of data subject can be limited in accordance with the DPA.

C. Storage, Retention and Destruction

The LGU will 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 LGU will implement appropriate security measures in storing all Personal Data, whether manually or electronically collected, and depending on the nature of the information.

Unless otherwise restricted by any law or regulation, including the provisions of R.A. No. 9470, otherwise known as the "National Archives of the Philippines Act of 2007," Personal Data shall be stored and retained only for as long as necessary to fulfill the purposes for which they were collected. After the fulfillment of its purpose or storage and retention period, Personal Data shall be disposed of or destroyed in a manner that prevents loss, misuse or unauthorized access or use. The LGU shall:

a. Document actual application of its retention policies and disposal procedures;
b. Retain, store, erase, remove, dispose or destroy records, archives, and copies of records when no longer required for their purpose, in accordance with its retention policies; and
c. Ensure that Personal Data are not kept beyond the declared retention time unless there is a justified reason for doing so.

D. Disposal of Personal Data

Disposal of Personal Data shall be in a secure manner, and as may be provided by existing laws and regulations.

All physical copies of the Personal Data shall be disposed or destroyed using secure methods and in accordance with this Privacy Manual, prevailing law, rules, and regulations. All physical copies of confidential and internal-use only documents including documents containing the Personal Data for disposal shall be shredded prior to disposal. Public documents may be used for recycling purposes but should ultimately be shredded prior to disposal.

All electronic copies of Personal Data shall be disposed by means of encryption and/or hard deletion to ensure that any personal/sensitive/privileged data cannot be accessed by any unauthorized sources. Moreover, hard disk/s containing data which are already past their retention period are required to undergo physical destruction to permanently erase all data.

Access

Only authorized officials, staff, personnel, and employees of the LGU, for legitimate use, shall have access to Personal Data. The LGU shall implement access controls, through organizational, physical, and technical measures, so that only authorized officials, staff, personnel, and employees of the LGU will have access to Personal Data for legitimate use, review, and updating, or disposal, as the case may be.

Subject to exceptions allowed by the law and regulations, Data Subjects shall be informed of their rights with respect to their Personal Data and how they may review, access, update, and correct their Personal Data, as well as secure a portable copy of thereof.

E. Disclosure and Sharing

All public officials (whether elected or appointed), their staff, and personnel of the LGU (whether permanent, casual, job order or contractual) shall maintain the confidentiality and secrecy of all Personal Data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations. For such purpose, all officials, staff, personnel, or employees of the LGU having access to Personal Data shall be required to execute a Non-Disclosure or Confidentiality Agreement.

Disclosure and/or sharing of Personal Data shall be subject, but not limited to, the following parameters:

1. *Intra-Access to Personal Data* — In the course of the LGU's operations, its duly-authorized officials, staff, personnel, and employees may have access and, from time-to-time, use and/or share Personal Data among various offices within the LGU. Provided, however, that the use and sharing thereof are necessary in order to carry out the officer's, employee's or personnel's functions pursuant to the Department's mandates and functions. No Personal Data may be shared to any officer, employee or personnel of the Department without an applicable Confidentiality and Non-Disclosure Agreement or Undertaking in place.

2. *Sharing of Personal Data Pursuant to Lawful Orders and Directives from Competent Authority* — Personal Data may be disclosed, through various legal processes or by court order, to law enforcement, regulatory agencies or third parties. Any Personal Data shared pursuant to lawful orders and directives shall be properly documented and accounted for by the concerned Office or Department. Should there be any such process or order, the Data Subject shall be informed to give ample opportunity to dispute such process or order.

3. *Sharing of Personal Data Pursuant to Outsourcing and Subcontracting Agreements.* – – Subject to the requirements and limitations under the DPA, the LGU may subcontract or outsource the processing of Personal Data. For this purpose, the LGU shall execute an Outsourcing Agreement, as well as other contractual or reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the Personal Data processed, to prevent its use for unauthorized purposes, and strictly comply with the requirements of the DPA, its IRR, other applicable laws for processing of Personal Data, and other issuances of the NPC.

   Any subcontracting or outsourcing of processing shall be governed by the afore-mentioned Outsourcing Agreement that shall bind the processor to the following commitments:

   i. Process the Personal Data only upon the documented instructions of the LGU, including transfers of Personal Data to another country or an international organization, unless such transfer is authorized by law;
   ii. Ensure that an obligation of confidentiality is imposed on persons authorized to process the Personal Data;
   iii. Implement appropriate security measures and comply with the DPA, its IRR Rules, and other issuances of the NPC;
   iv. Not engage another processor without prior instruction from the LGU. Provided, that any such arrangement shall ensure that the same obligations for data protection under contract or legal act are implemented, taking into account the nature of the processing;

v. Assist the LGU, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;

vi. Assist the LGU in ensuring compliance with the DPA, its IRR, other relevant laws, and other issuances of the NPC, taking into account the nature of processing and the information available to the PIP;

vii. At the choice of the LGU, delete or return to the LGU all Personal Data after the end of the provision of services relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the DPA or another law;

viii. Make available to the LGU all information necessary to demonstrate compliance with the obligations laid down in the DPA, and allow for and contribute to audits, including inspections, conducted by the LGU or another auditor mandated by the latter;

ix. Immediately inform the LGU if, in its opinion, an instruction infringes the DPA, its IRR, or any other issuance of the NPC.

x. Comply with the requirements of the DPA and its IRR, other applicable laws, and any other issuance of the NPC, in addition to obligations provided the Outsourcing Agreement, or other legal act executed by the LGU with the PIP.

The subcontracting and/or outsourcing of the processing of the Personal Data to any third party shall not relieve the concerned official/s, staff, personnel, and employee/s from full liability and accountability for ensuring compliance with the law and this Privacy Manual.

4. *Data Sharing to Third Parties and Other Government Agencies* — For purposes of fulfilling its mandates and functions, or for provision of public service, the LGU may disclose or share the Personal Data to a third party or another government agency, provided that the disclosure or sharing thereof is in accordance with the provisions of the DPA, its IRR, other applicable laws for processing of Personal Data, and other issuances of the NPC, and a Data Sharing Agreement, for such purpose, is duly entered into by the LGU and the said third party and/or government agency.

In any case, Personal Data under the custody of the LGU shall be disclosed and/or shared only pursuant to a lawful purpose, and to authorized recipients of such data especially if there is a Data Sharing or an Outsourcing Agreement duly entered for such purpose.

VI. SECURITY MEASURES

The LGU shall take appropriate and reasonable precaution to protect Personal Data from unauthorized access, disclosure, use, alteration, destruction, damage, loss or processing. For this purpose, the following measures are in place:

A. Organizational Security Measures

1. **Data Protection Officer**—The designated DPO is **Atty. Jose Elmer Y. Teodoro**, who is concurrently serving as the City Legal Officer of the Local Government Unit of City of San Fernando, Pampanga (LGU-CSFP). To support the DPO in performing his duties as such, there is a designated COP from every Department of the LGU. The DPO and the COPs may be reached thru: email address : dpo@cityofsanfernando.gov.ph or office address: at the **City Legal Office, Ground Floor, Heroes Hall, Brgy. San Juan, City of San Fernando, Pampanga**.

The DPO, with the assistance of the duly designated COPs, and/or any other responsible personnel with similar functions, shall be responsible for:

a. Overseeing and monitoring the compliance of the LGU with the DPA, its IRR, and other related policies, including the conduct of a PIA, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure;
b. Formulating, maintaining, monitoring, reviewing, and updating the LGU's privacy policies and information security programs;
c. Documenting, implementing, enforcing, monitoring, and updating privacy policies and information security programs of the LGU;
d. Establishing standards for the classification of Personal Data;
e. Determining the required level of protection for each classification of Personal Data; and
f. Initiating actions for the training of personnel on updates and developments in data privacy and security.

2. Adoption of a Comprehensive Information Security Program

The LGU's security measures shall be continuously developed, documented, approved, and implemented. The measures shall include administrative, technical, and physical safeguards to protect Personal Data from unauthorized access, disclosure, use, alteration, destruction, damage, loss or processing, such as, but not limited to:

a. Periodic risk assessments;
b. Identification and documentation of the security requirements of authorized users;
c. Development and updating of access policies, controls, and procedures with respect to Personal Data, whether or not they are in active use by the LGU;
d. Assignment of responsibility and accountability for security;
e. Assignment of responsibility and accountability for system changes and maintenance;
f. Implementing system software upgrades and patches;
g. Testing, evaluating and authorizing system components before implementation, and thereafter regularly on an annual basis;
h. Addressing complaints and requests relating to security issues;
i. Development of protocols for handling errors and omissions, security breaches, and other incidents;
j. Development of procedures and protocols to detect actual and attempted attacks or intrusions into system and to proactively test security procedures;
k. Allocating training and other resources to support its security policies;
l. Development of disaster recovery plans and related testing; and
m. Requiring users, management, and third parties to confirm their understanding of, and agreement to comply with the LGU's security policies and procedures, including the execution of a Non-Disclosure or Confidentiality Agreement, a Data Sharing Agreement or an Outsourcing Agreement, whichever is applicable.

3. Conduct of trainings or seminars to keep personnel, especially the Data Protection Officer updated *vis-à-vis* developments in data privacy and security

The LGU shall sponsor a mandatory training on data privacy and security at least once a year for LGU representatives or personnel directly involved in the

processing of personal data management. The LGU shall ensure their attendance and participation in relevant training and orientations, as often as necessary.

4. Conduct of Privacy Impact Assessment

The LGU shall conduct a PIA relative to all service/s, program/s, activity/ies, and/or benefit/s involving the processing of Personal Data. It may choose to outsource the conduct a PIA to a third party, subject to the requirements of the DPA and other applicable data protection laws.

The PIA shall include an assessment of the documents, data processing system/s and policies used by various departments/offices of the City Government. It shall also incorporate the process of understanding the personal data flow, identifying and assessing threats and vulnerabilities, and proposing measures to address privacy risks.

5. Recording and documentation of activities carried out by the DPO/COP, or the LGU itself, to ensure compliance with the DPA, its IRR and other relevant policies

The LGU shall record or document its activities related to the DPA, its IRR, and other relevant policies.

6. Duty of Confidentiality

All officials, staff, personnel, or employees of the LGU having access to Personal Data shall be required to execute a Non-Disclosure or Confidentiality Agreement. 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, and must agree that:

i. He/she must treat all information, including Personal Data or information accessed as a result of or by virtue of his or her involvement with the LGU as strictly confidential;
ii. He/she shall use the information or Personal Data only as may be necessary to perform his/her duties as an officer, personnel or employee of the LGU;
iii. He/she shall not disclose or allow the disclosure of information or Personal Data to unauthorized persons;
iv. He/she must return all the LGU's properties and documents, including Personal Data or information and copies thereof, their excerpts, summaries or briefs containing or referring to said Personal Data or information upon the end of his/her term, employment, contract or involvement with the LGU;
v. The duty to protect the confidentiality of information does not end at the time of termination of his/her term, employment, contract or involvement; and
vi. He/she has a continuing obligation to maintain confidentiality of Personal Data or information that he/she acquired in the course of or during his/her employment at the LGU, even after the termination of his/her term, employment, contract or involvement with the LGU.

7. Periodic Review of Privacy Manual

This Manual shall be periodically reviewed and evaluated. Privacy and security policies and practices within the LGU shall be updated to remain consistent with current data privacy best practices.

B. Physical Security Measures

1. Format of data to be collected

Personal data in the custody of the LGU may be in digital/electronic format and paper-based/physical format. Usual Personal Data to be collected are, but not limited to, the name, contact details, address, date of birth, and other pertinent personal information relevant to the services, programs, activities, and benefits offered by the LGU.

2. Storage type and location, (e.g. filing cabinets, electronic storage system, personal data room/separate room or part of an existing room)

All Personal Data being processed by the LGU shall be stored in a data/record room of the concerned Office or Department of the LGU, where paper-based documents are kept in locked filing cabinets; while the digital/electronic files are stored in computers, sewers and/or storage devices provided and installed by the company.

The database servers of the information system are stored in the City Information and Communications Technology Office (CICTO) servers that are protected with firewall and security protocols. Unrecognized IP Addresses are blocked. Basic Personal Information are also encrypted.

3. Access procedure of agency personnel

Only authorized LGU representatives or personnel shall be allowed inside the data/record room or to directly access the digital/electronic files stored in computers/devices provided and installed by the LGU. For this purpose, they shall each be given a duplicate key to the room/access code to the computers/devices. Other personnel may be granted access to the data record room or computers/devices upon filing of an access request form with the DPO /COP and the latter's approval thereof or pursuant to a Data Sharing Agreement.

4. Monitoring and limitation of access to room or facility

All LGU representative or personnel authorized to enter and access the data room or facility or computer must fill out and register with the online registration platform of the LGU, and/or a logbook placed at the entrance of the room. They shall indicate the date, time, duration and purpose of each access.

The CICTO's server administrators are always monitoring the access of the server, hence, once detected that a certain malicious action or access has been made, a technical action will be done.

5. Design of office space/work station

The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data. In case of personal fill up of

application, the LGU representative or personnel shall ensure the privacy of the Data Subject or that the document be away from prying eyes of third persons.

6. **Persons involved in processing and their duties and responsibilities**

Persons involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their own gadgets or storage device of any form when entering the data storage room. They are also not allowed to take out the said data whether stored in a physical document or data storage device without the appropriate authority from the DPO/COP.

7. **Modes of transfer of personal data within the LGU or to third parties**

Personal or physical transfer of documents containing the personal data shall be prioritized whenever possible. Transfers of Personal Data *via* electronic mail shall use a secure email facility / storage device with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal data.

8. **Retention and disposal procedure**

In relation to *Item V(c)* of this Privacy Manual, and unless otherwise restricted by any policy, law, or regulation, including the provisions of National Archives of the Philippines Act of 2007, the retention of the Personal Data collected by the LGU shall be for a period of one (1) year from the date of its processing or until the fulfillment of its purpose has been achieved.

Upon expiration of such period or whenever the data is no longer necessary to be stored and kept, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology or means.

C. Technical Security Measures

1. **Monitoring for Security Breaches**

The LGU shall use an intrusion detection system to monitor security breaches and alert it of any attempt to interrupt or disturb the system.

2. **Security features of the software/s and applications used**

The LGU shall first review and evaluate software applications before the installation thereof in its computers/devices to ensure the compatibility of security features with overall operations.

3. **Periodic Risk Assessment**

To protect computerized and digitized data or information, a periodic risk assessment shall be implemented by the LGU.

4. **Process for regular testing. Assessment and evaluation of effectiveness of security measures**

The LGU shall review security policies, conduct vulnerability assessments and perform penetration testing within the LGU on regular schedule (quarterly) to be prescribed by the appropriate office.

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

Transfer of personal data via electronic mail shall use a secure email facility with encryption of data, including any or all attachment.

Each LGU representative or personnel with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication.

Moreover, saving of files to portable storage (external hard drives, USB disks, etc.) shall be discouraged within the departments/offices of the City Government. An allocated network drive shall always be preferred to saving files locally to an equipment.

6. Protection of Data Related to Data Processing and those Related to Theft, Malicious Destruction, Corruption of Hardware and Software

The protection of data relating to processing, theft, malicious destruction, and corruption of hardware and software will be covered by programs and software routines based on existing cybersecurity policies. The existing Cybersecurity Policy shall be constantly reviewed and updated by the CICTO in coordination with the DPCC and other concerned Offices and Departments of the LGU. Said Cybersecurity Policies shall cover protection against theft, malicious destruction and corruption of hardware and software.

7. Protection Against Common Security Risks

Among the common security risks related to computerized and digitized Personal Data or Information are hacking, viruses, cookies, phishing, and social engineering. To address the above-enumerated risks, the following shall be instituted, monitored, and controlled by the LGU:

i. Firewall and antivirus subscriptions shall, at all times, be up-to-date and installed in all systems, and devices with access to Personal Data and Information possessed by the LGU;
ii. Secured Socket Layer (SSL) should be enabled at all times for both e-mail system and websites associated with the LGU;
iii. All inbound external internet traffic must pass through a configured firewall and network level intrusion detection system in order to prevent unauthorized traffic and scan for inappropriate and malicious content. The LGU reserves the right to monitor internet connectivity in order to detect misuse;
iv. Vulnerability assessment and penetration testing of systems shall be conducted at least once a year;
v. A proper back-up strategy and recovery plan to protect all Personal data and Information shall be implemented; and
vi. Mandatory training of all stakeholders on the proper disclosure of Personal Data shall be regularly conducted.

8. Access Control

The LGU shall enforce access control through the use of centrally-administered systems, with modification to access rights logged accordingly, and applying the following guidelines:

i. All confidential data must be protected via access controls through the use of authentication protocols and/or encryption keys to prevent security breach;
ii. Access to passwords, encryption keys, Personal Data and information shall be in accordance with the LGU's Encryption Policy and tracked, identifying who accessed it and when it was accessed;
iii. Access to systems or applications with access to Personal Data or Information requires the approval of the appropriate authority;
iv. Access to data by officers, employees or personnel of the LGU not otherwise granted authority must be approved by the appropriate authority;
v. All parties accessing the LGU's information processing systems must utilize a unique account in order to link actions to an individual;
vi. Built-in administration accounts shall not be used by an individual;
vii. Redundant accounts will be regularly reviewed and disabled/removed;
viii. All user-accounts must be disabled when no longer used by an individual;
ix. Access rights must be revoked when no longer required in the exercise of functions and powers of the LGU;
x. Sessions used by individuals shall be restricted to a maximum idle-time to reduce opportunity for unauthorized access. Systems will lock when maximum idle-time has been reached;
xi. Applications used to facilitate information processing shall support unique accounts and least privilege permissions; and
xii. Only officers, employees or personnel who are aware of information and security policies and procedures of the LGU shall be allowed access to Personal Data and Information.

9. Use of emails

In order to protect Personal Data and Information when using emails, the following shall be observed:

i. All officers, personnel, and employees shall at all times use only the official email assigned to them by the LGU for all official communications;
ii. All inbound external emails must pass through a mail relay that scans for inappropriate content and viruses;
iii. All outbound emails must be scanned for viruses;
iv. The LGU reserves the right to monitor emails to detect misuse; and
v. Mechanism shall be in place to detect and filter malicious email content and floods of unwanted messages are received.

10. Passwords

The LGU shall implement the following to control access to information processing systems:

i. Access to the LGU's information processing systems must be controlled, at the minimum, by combination of a username and password;
ii. All third-party supplied accounts will have their passwords changed prior to being used in the LGU's system;
iii. Initial passwords shall be changed upon first use;
iv. Passwords shall be changed periodically. Should an account be compromised, an immediate change shall be required;
v. Password complexity must be enforced, requiring minimum password length and a combination of alpha-numeric, upper/lower case and special characters; and
vi. Passwords should not be reused.

11. Back-Up System

Personal Data and Information shall be backed up at regular intervals and before any major system changes, and configured according to the system backup policy and associated documentation.

The backup system must be able to verify that the backup process was successful to ensure the data can be restored properly.

Backup arrangements for individual systems shall also meet the requirements of the disaster recovery and business continuity policy and any associated plans.

12. System Monitoring and Vulnerability Scanning

i. System Monitoring.—To ensure that the ICT security controls of the LGU are effective and to identify security vulnerabilities to minimize potential risk impact, the systems, servers, and network infrastructure components shall be configured to the LGU's build standards for system hardening.

Network and host-based intrusion detection system/software shall be deployed to monitor for key events to indicate and alert upon malicious activity.

ii. Vulnerability Scanning.—Vulnerability scans are conducted per the LGU's process and schedule as defined in the relevant documentation, with remediation of any identified vulnerabilities performed within the appropriate time frame based on severity.

iii. Process for Regularly Resting, Assessment, and Evaluation of Effectiveness of Security Measures.—The LGU shall review security policies, conduct vulnerability assessments, and perform penetration testing within the LGU.

iv. Encryption, Authentication Process, and Other Technical Security Measures that Control and Limit Access to Personal Data.—Each officer, employee or personnel with access to Personal Data shall verify his or her identity using a secure encrypted link and multi-level authentication.

VII. BREACH AND SECURITY INCIDENTS

1. Creation of a Data Breach Response Team

A Data Breach Response Team (DBRT) shall be headed by the DPO and shall be composed of the following as its members:

- City Administrator
- City Legal Officer
- City Human Resource Management Officer
- City Information and Communications Technology Officer
- Chief, Internal Control Division
- Overall COP

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

2. **Measured to prevent and minimize occurrence of breach and security incidents**

The LGU shall regularly conduct a PIA to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of personal data are mandated to attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the LGU.

3. **Procedure for recovery and restoration of personal data**

The LGU shall always maintain a backup file for all Personal Data under its custody. In the event of a security incident or 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.

4. **Notification Protocol**

The DPO, as the Head of the DBRT, shall inform the head of the concerned Department/s and/or Office/s of the need to notify the NPC and the Data Subjects affected by the incident or breach within the period prescribed by law. Thereafter, the Head of the concerned Department/s and/or Office/s shall notify the DPO of their action taken and the response of the recipient of the notice within three (3) days therefrom.

5. **Documentation and reporting procedure of security incidents or a personal data breach**

The DBRT shall prepare a detailed documentation or report of every incident or breach encountered, as well as an annual report, to be submitted to the undersigned and the NPC, within the prescribed period.

In relation to the foregoing, the LGU shall publish a Data Breach Management Manual which shall specify the provisions, details, and procedures on how to act on data breaches and incidents.

VIII. RIGHTS OF DATA SUBJECTS

The LGU shall not only ensure that all Data Subjects shall be fully informed of their data privacy rights under the DPA, relevant laws, rules and regulations, and issuances of the NPC,

but also implement effective measures for the protection of such rights. The following rights of the Data Subject with respect to their Personal Data are recognized by the Department:

1. **Right to be Informed**—The LGU shall ensure that its Privacy Policy made accessible to the Data Subject before entry of his or her Personal Data into the LGU's processing system is sufficiently informative for him or her to know:

    i. Description of the personal data to be entered into the system;
    ii. Purposes for which they are being or will be processed;
    iii. Basis of processing, when processing is not based on the consent of the data subject;
    iv. Scope and method of the personal data processing;
    v. The recipients or classes of recipients to whom the personal data are or may be disclosed;
    vi. Methods utilized for automated access, if applicable and if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
    vii. The identity and contact details of the personal data controller or its representative;
    viii. The period for which the information will be stored; and
    ix. The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.

2. **Right to Object**—The Data Subject may at any time notify the LGU of his or her desire to withhold consent to the processing of Personal Data for any reason or in case of changes in the information supplied or declared to him or her in the preceding paragraph. The LGU shall cease the processing of a Data Subject's Personal Data as soon as it receives a valid notice that the Data Subject withholds his or her consent to the processing of his or her data in case the processing is based on consent. The right to object shall not apply if the processing of his or her Personal Data has basis other than consent such as but not limited to the following:

    i. The Personal Data is needed pursuant to a subpoena;
    ii. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
    iii. The information is being collected and processed as a result of a legal obligation.

3. **Right to Access**—The LGU may give the Data Subject access to the following information upon receipt of a written demand addressed to the DPO:

    i. Contents of his or her Personal Data that were processed;
    ii. Sources from which Personal Data were obtained;
    iii. Names and addresses of recipients of the Personal Data;
    iv. Manner by which such data were processed;
    v. Reasons for the disclosure of the Personal Data to recipients, if any;

vi. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the Data Subject;
vii. Date when his or her Personal Data concerning the data subject were last accessed and modified; and
viii. The designation, name or identity, and address of the PIC.

4. **Right to Rectification**—The Data Subject may report any discovered inaccuracy or error in his or her Personal Data being processed by the LGU. Upon confirmation and verification, the LGU, through the DPO shall enact measures to correct the inaccuracy or error in its system provided that the request is not vexatious or unreasonable. The Data Subject has the right to dispute the inaccuracy or error in the personal data and have the PIC correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. Upon correction or rectification of the Personal Data, the LGU shall ensure, the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: Provided, That recipients or third parties who have previously received such processed Personal Data shall be informed of its inaccuracy and its rectification, upon reasonable request of the Data Subject.

5. **Right to Erasure or Blocking**—The Data Subject may request the suspension, withdrawal, blocking, removal or destruction of his or her Personal Data from the LGU's system. This right may be exercised upon discovery and substantial proof of any of the following:

i. The Personal Data is incomplete, outdated, false, or unlawfully obtained;
ii. The Personal Data is being used for purpose not authorized by the Data Subject;
iii. The Personal Data is no longer necessary for the purposes for which they were collected;
iv. The Data Subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
v. The Personal Data concerns private information that is prejudicial to Data Subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
vi. The processing is unlawful;
vii. The LGU or its PIP violated the rights of the Data Subject; and
viii. The LGU may notify third parties who have previously received such processed personal information.

IX. INQUIRIES AND COMPLAINTS

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the LGU, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the LGU at dpo@cityofsanfernando.gov.ph and briefly discuss the inquiry, together with their contact details for reference.

Complaints shall be filed in three (3) printed copies, or sent to dpo@cityofsanfernando.gov.ph. The concerned department or unit shall confirm with the complainant its receipt of the complaint within 24 hours.

The issuance of Resolution of the complaint shall be no longer than thirty (30) days from the date of acknowledgment, unless an extension is deemed necessary based on its complexity.

X. INQUIRIES AND COMPLAINTS

Non-compliance by any official, staff, or personnel of the LGU (whether permanent, casual, job order or contractual) with this Privacy Manual shall be communicated immediately to the DPCC. The DPCC shall immediately conduct and independent investigation on any report of noncompliance with this Privacy Manual. If found liable, the violator may be subjected to administrative sanctions. Further, all acts punishable under the DPA, its IRR, and prevailing laws and regulations shall be reported to the NPC for appropriate action.

XI. AMENDMENTS

The provisions of this Privacy Manual, shall, at all times, be subject to the prevailing issuances of the LGU on data privacy. This Privacy Manual may subsequently be amended or modified by the LGU. Any amendment, modification, or revision to this Privacy Manual shall become valid and binding to the public and/or all interested parties after the publication of the amended, modified, or revised Privacy Manual.

XII. SEVERABILITY

If any provision contained herein is invalid, illegal or unenforceable in any respect under any applicable law or decision, the validity, legality, and enforceability of the remaining provisions shall not be affected or impaired in any way. The LGU shall, so far as practicable, execute such additional documents in order to give effect to any provision hereof which is determined to be invalid, illegal, or unenforceable.

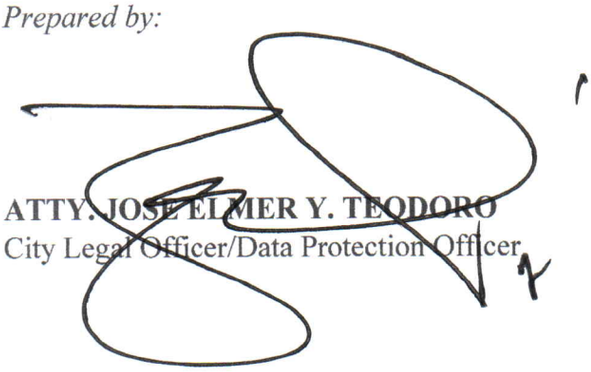
XIII. EFFECTIVITY

This Privacy Manual shall be effective this ___ day of _____, until revoked or amended.

XIV. ANNEXES

1. Consent Form
2. Privacy Notice

Prepared by:



ATTY. JOSE ELMER Y. TEODORO
City Legal Officer/Data Protection Officer

Approved by:

ENGR. NELSON G. LINGAT, DPA
City Administrator