AP SECURITIES, INCORPORATED
(Member of Philippine Stock Exchange - PSE)

DATA PRIVACY MANUAL

DATA PRIVACY MANUAL OF AP SECURITIES, INCORPORATED

I. INTRODUCTION

This Privacy Manual of **AP SECURITIES, INCORPORATED** is hereby adopted in compliance with Republic Act. No. 10173 entitled "An Act Protecting Individual Personal Information and Communication System in the Government and the Private Sector, Creating for this Purpose a **National Privacy Commission**, and for other Purposes" or otherwise known as the **"Data Privacy Act of 2012"**, its Implementing Rules and Regulations, relevant policies and issuances of the **National Privacy Commission ("NPC").**

The **Data Privacy Act ("DPA")** and its Implementing Rules and Regulations ("IRR") provide the following:

1. Protection of individual's right to privacy of his personal information and sensitive personal information **("Personal Data")** while ensuring the free flow of information in order to promote innovation and growth;

2. Regulation in the processing of personal information and, in certain cases, processing of sensitive personal information and privileged information;

3. Creation of the **NPC** tasked to implement the provisions of the **DPA** and its **IRR** and to ensure country's compliance with international standards for data protection;

4. Security of personal information through the implementation of reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal and sensitive personal information.

APS respects, values, and protects the data privacy rights of individuals and ensures that all personal information and sensitive personal information ("Personal Data") collected are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality. APS collects Personal Data from the following:

a. APS directors, stockholders, officials, employees, interns, on-the-job trainees, agents, and consultant/s;

b. Client's;

c. Banks' representatives;

d. Directors, officials, and pertinent employees of (i) Philippine Depository & Trust Corp. **("PDTC")**; (ii) Securities Clearing Corporation of the Philippines **("SCCP")**; (iii) The Philippine Stock Exchange, Inc. **("PSE")**; (iv) Capital Markets Integrity Corporation **("CMIC")**; (v) Philippine Association of Securities Brokers Dealers, Inc. **("PASBDI")**; (vi) Securities Investors Protection Fund **("SIPF")**; (vii) listed companies and other corporations or entities that the APS may deal with; (viii) Trading Participants **("TP")**; (ix) Securities and Exchange Commission **("SEC")**; (x) Anti Money Laundering and its Secretariat; **(AMLA**)(xi) National Privacy Commission **("NPC")**; (xii) Bureau of Internal Revenue **("BIR")**; (xiii) other government agencies; and (xiv) representatives of trade.

This Privacy Manual provides APS data protection and security measures and may serve as guide in exercising rights of a data subject under the **DPA.**

II. DEFINITION OF TERMS

The DPA and its IRR define the following:

a. **"DATA SUBJECT"** – refers to an individual whose personal, sensitive personal or privileged information is processed by the organization. It may refer to officers, employees, consultants, and clients of this organization.

b. **"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.

Examples of Personal information are: name, home, address or office address, email address, birth date, birth place, telephone number, place of work, gender, location of an individual at a particular time, IP address, country of citizenship, citizenship status, payroll and benefits information and other identifying information.

c. **"PERSONAL DATA"** refers to both personal information and sensitive personal information.

d. **"PERSONAL DATA BREACH"** – refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed;

e. **"PERSONAL INFORMATION PROCESSOR"** – refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

f. **"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.

g. **"PRIVILEGED INFORMATION"** - refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

h. **" 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;

i. **"SENSITIVE PERSONAL INFORMATION"** - refers to personal information:

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

(ii) 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;

(iii) 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

(iv) Specifically established by an executive order or an act of Congress to be kept classified.

Examples of sensitive personal information are: banks and credit/debit card numbers, websites visited, materials downloaded, any other information reflecting preferences and behavior of an individual, grievance information, and leave of absence reason.

III. SCOPE AND LIMITATIONS

All personnel of APS, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Privacy Manual. This Privacy Manual is an internal issuance and is meant for the use and application of the APS staff or personnel and is not intended for publication.

IV. PROCESSING OF PERSONAL DATA

APS, in the processing of personal information, implements and observes the following applicable provisions of Section 12 of the DPA which provides: " The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

a. The data subject has given his or her consent;

b. The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data prior to entering into a contract;

c. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

d. The processing is necessary to protect vitally important interests of the data subject, including life and health;

e. The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or

f. The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedom of the data subject which require protection under the Philippine Constitution. (Underscoring supplied)

In the processing of sensitive personal information, the APS implements and observes the following applicable provisions of Section 13 of the DPA which states that: " The processing of sensitive personal information and privileged personal information shall be prohibited, except in the following cases

a. The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

b. The processing of the same is provided for by existing laws and regulations: Provided, that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

c. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing

d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided , that such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, that the sensitive personal information are not transferred to third parties: Provided further, that the sensitive personal information are not transferred to third parties: Provided finally, that consent of the data subject was obtained prior to processing.

e. The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

f. The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

A. COLLECTION

The APS collection of Personal Data is done by lawful means and for lawful purposes and is directly related and necessary to the nature, functions, and purposes of the APS as a securities broker dealer.

As a securities broker dealer, the APS collects the following Personal Data:

(a) Client's name, Tax Identification number, name of spouse, home and business telephone numbers, business fax number, passport information or government issued Identification card and such other information that the APS may see fit;

(b) Basic contact information of :

(i) officials and pertinent employees of PSE, CMIC, and SCCP;

(ii) officials and employees of SIPF, PASBDI;

(iii) officials and pertinent employees of other TPs;

(iv) chairman, commissioners, directors, and whenever necessary, officers/employees of SEC;

(v) officers and employees of applicable government agencies and LGU;

(vi) officers and pertinent employees of LCs;

(vii) representatives of trade suppliers; and

(viii) individuals who transact with the APS. The basic contact information consists of full names, addresses or email addresses, place of work, gender, and contact numbers.

Likewise, the APS also collects Personal Data from its members of the Board of Directors, officials, and employees, regardless of the type of employment or contractual arrangement, including on-the-job trainees and applicants for vacant positions. Personal Data are collected through documents submitted or gathered in relation to job application or.

B. USE

The APS uses Personal Data collected for purposes of :

(i) complying with the laws, rules and regulations issued by PSE, CMIC, SCCP, SEC and other government agencies,

(ii) for purposes of its operations as securities, broker, dealer, and

(iii) for documentation purposes.

C. STORAGE, RETENTION AND DESTRUCTION

The APS shall ensure that Personal Data under its custody, whether in paper or electronic format, are protected against any accidental or unlawful destruction, alteration, and disclosure, including against any other unlawful processing. The APS implements appropriate security measures in storing collected Personal Data, depending on the nature of the information, and Personal Data whether in paper or electronic format will be safely destroyed through secure means, after the lapse of the retention period provided by law, rules or regulations or as determined by the APS..

D. ACCESS

Due to the sensitive and confidential nature of the Personal Data under the custody of the APS, only the authorized representatives of the APS shall be allowed to access such Personal Data for any purpose, except:

(i) for those contrary to law, public policy, public order or morals, or

(ii) when access by others is required or allowed by law or rules and regulations of the SEC, CMIC, or PSE, or

(iii) when required by exigency of the business and operation of the APS as a securities broker dealer.

E. DISCLOSURE AND SHARING

All employees, officers, and directors of the APS shall maintain the confidentiality and secrecy of all Personal Data that come to their knowledge and possession, even after resignation or termination of contract or other contractual relations, unless otherwise required to be disclosed by law, its rules and regulations, or rules and regulations of the PSE, CMIC, or SCCP, or with the consent of the Data Subject.

V. SECURITY MEASURES

As a personal information controller, the APS implements reasonable and appropriate physical, technical and organizational measures for the protection of Personal Data. Security measures aim to maintain the availability, integrity and confidentiality of Personal Data and protect them against natural dangers such

as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

A. ORGANIZATION SECURITY MEASURES

1. DATA PROTECTION OFFICER

The APS designated **Mr. Danny Alqueza** as its Protection Officer (DPO).

2. FUNCTIONS OF THE DPO

The following are the functions of the DPO:

a. Monitor compliance of the APS with the DPA, its IRR, issuances by the NPC and other applicable laws and policies;

   (i) Collect information to identify the processing operations, activities, measures, projects, programs, or systems of the APS, 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 providers;
   (iii) Inform, advise, and issue recommendations to the APS;
   (iv) Ascertain renewal of accreditations or certifications necessary to maintain the required standards in Personal Data processing; and
   (v) Advice the APS 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 Assessment ("PIA") relative to activities, measures, projects, programs or systems of the APS;

c. Advise the APS 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 APS, 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 APS, including all relevant laws, rules, and regulations, and issuances of the NPC;

f. Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the APS relating to privacy and data protection by adopting a privacy by design approach;

g. Serve as the contact person of the APS vis-à-vis data subjects, the NPC, and other authorities in all matters concerning data privacy or security issues or concerns;

h. Cooperate, coordinate, and seek advice of the NPC regarding matters concerning data privacy and security; and

i. Perform other duties and tasks that may be assigned by the APS that will further the interests of data privacy and security and uphold the rights of the data subjects.

3. Conduct of trainings, recording and documentations of compliance

The APS shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of Personal Data, the management, through the DPO, shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

The APS will keep a recording and documentation of activities carried out by the DPO, or the APS itself, to ensure compliance with the DPA, its IRR and other relevant policies or issuances of the NPC.

4. Conduct of Privacy Impact Assessment

The APS shall conduct a PIA relative to all activities, projects and systems involving the processing of Personal Data. The PIA may be conducted on a specific project or system when deemed to be necessary. The APS may outsource the conduct of the PIA to a third party.

5. Duty of Confidentiality

All employees and officers of the APS shall be required to sign confidentiality and non-disclosure agreement. All APS employees and officers with access to Personal Data shall operate and hold Personal Data under strict confidentiality if the same is not intended for public disclosure or unless such disclosure is required under the law, rules and regulations of the SEC, CMIC, or PSE or with the consent of the Data Subject.

6. Review of Privacy Manual

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

B. PHYSICAL SECURITY MEASURES

1. Format of Personal Data

Personal data in the custody of the APS are in digital or electronic format and paper based or physical format.

2. Storage type and location

All Personal Data in paper-based documents being processed by the APS are stored in designated storage areas or kept in locked filing cabinets while the digital or electronic files are safely stored in computers provided and installed by the APS with appropriate passwords which are changed on a regular basis.

3. Access procedure of APS personnel

Only authorized personnel shall be allowed inside the data room. For this purpose, they shall each be given a duplicate of the key to the room. Other personnel may be granted access to the room upon filing of an access request form with the Data Protection Officer and the latter's approval thereof.

4. Monitoring and limitations of access

Physical access is restricted to authorized personnel and any visitor is escorted by an authorized individual while in the office or secure area. All authorized personnel who seek to access the stored Personal Data must fill out and register access details in a logbook. They shall indicate the date, time, duration and purpose of each access.

5. Design of office space/work station

For purposes of ensuring privacy of Personal Data, the computers used by APS personnel are positioned with considerable spaces between them to maintain privacy and protect the

processing of Personal Data. A nightly closing protocol requires employees and officials of the APS to log out of all computers.

6. Person 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. Moreover, all employees and officers of the APS with access to Personal Data shall operate and hold Personal Data under strict confidentiality if the same is not intended for public disclosure or unless such disclosure is required under the law or its rules and regulations or rules and regulations of SEC, CMIC, PSE, or SCCP.

7. Modes of transfer of personal data within the organization, or to third parties

Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal data, unless with the consent of the data subjects.

8. Retention and disposal procedure

The APS shall retain the Personal Data for a period allowed by law, rules and regulations. Upon expiration of such period, all physical and electronic copies of the Personal Data shall be destroyed and disposed of using secure technology.

C. TECHNICAL SECURITY MEASURES

The APS shall implement technical security measures to make sure that there are appropriate and sufficient safeguards to secure the processing of Personal Data, particularly the computer network in place, including encryption and authentication processes that control and limit access. They include the following, among others:

1. Monitoring for security breaches

The APS may use an intrusion detection system to monitor security breaches and alert the APS of any attempt to interrupt or disturb the system. The APS installs anti-virus software to computers and laptops that regularly access the internet and uses firewalls and anti-virus/anti-spyware software to protect systems that are accessible from the internet. The systems that are exposed to the Internet such as the web servers and their software or servers supporting sensitive applications are removed or disabled of unnecessary services

and applications and with properly configured user authentication. The APS regularly reads the firewall logs to monitor security breaches or any unauthorized attempt to access the network of the APS.

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

   The APS reviews and evaluates software applications before the installation thereof in computers and devices of the APS to ensure the compatibility of security features with overall operations and to ensure privacy protection of Personal Data stored in said computers.

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

   The APS reviews security policies, conduct vulnerability assessments, and perform penetration testing within the APS on regular schedule to be prescribed by the appropriate department or unit.

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

   The APS personnel with access to Personal data shall verify his or her identity using a secure encrypted link and multi-level authentication.

V. BREACH AND SECURITY INCIDENTS

1. **Creation of a Data Breach Response Team**

   A Data Breach Response Team comprising of {five (5) officers – NAME OF THE TEAM} 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. **Measures to prevent and minimize occurrence of breach and security incidents**

   The APS shall regularly conduct a Privacy Impact Assessment 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 must attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the organization.

3. Procedure for recovery and restoration of personal data

The APS 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 Head of the Data Breach Response Team shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the head of the Data Breach Response Team. Such notification shall be done within seventy two (72) hours upon knowledge of, or when there is reasonable belief by the APS that a Personal Data breach requiring notification has occurred. A breach shall be subject to notification requirements under the following conditions.

a. The compromised data involves sensitive personal information or other information that may be used to enable identity fraud;
b. There is reason to believe that the information may have been acquired by an unauthorized person; and
c. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The report shall contain the following:

a. Description of the nature of the breach;
b. Sensitive personal information possibly involved;
c. Measures taken by the entity to address the breach;
d. Measures taken to reduce the harm or negative consequences of the breach; and
e. Name of the DPO or representatives of the APS, including their contact details, from whom the data subject can obtain additional information about the breach and any assistance to be provided to the affected data subjects.

5. Documentation and reporting procedure of security incidents or a Personal Data breach

The Data Breach Response Team shall prepare a detailed documentation of all security incidents and Personal Data breaches, including those not covered by the notification

requirements. In the case of Personal Data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the APS. In other security incidents not involving Personal Data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the NPC. A general summary of the reports shall be submitted to the NPC annually.

VI. INQUIRIES AND COMPLAINTS

Every data subject has the right to reasonable access to his or her Personal Data being processed by the personal information controller or personal information processor. Other available rights include: (1) right to dispute the inaccuracy or error in the Personal Data; (2) right to request the suspension, withdrawal, blocking, removal or destruction of Personal Data; and (3) right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of Personal Data. Accordingly, there must be a procedure for inquiries and complaints that will specify the means through which concerns, documents, or forms submitted to the organization shall be received and acted upon. The data subject may write to the APS at _____ to discuss the inquiry, together with their contact details for reference.

Complaints shall be filed in three (3) printed copies or sent to _____. The concerned department or unit of the APS shall confirm with complainant its receipt of the complaint.

VII. EFFECTIVITY

This Privacy Manual takes effect on _____until revoked or amended.

Prepared by:

ABIGAIL C. LORICA

Approved by:

WILMA C. CRISOSTOMO
President/Nominee