	DATA PRIVACY MANUAL				
Document No.:	**CPGI-DPM**	Revision No.:	**000**	Issuance Date:	**May 08, 2019**
Department:	**Corporate Compliance**			Effective Date:	**May 08, 2019**
DATA PRIVACY MANUAL FOR CENTURY PROPERTIES GROUP, INC.					

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Century Properties Group, Inc. (the "**Group**") endeavors to meet leading standards and regulations for data protection and privacy. The Group respects and values data privacy rights of data subjects, and makes sure that all personal data collected from the data subjects are processed in accordance to the general principles of transparency, legitimate purpose, and proportionality. While our reasons are founded in ethical and corporate responsibility, our privacy practices as outlined in this policy facilitate the following

- *Good Corporate Citizenship:* A sound Privacy Policy is emblematic of reliable corporate citizens that respect data subjects' privacy.
- *Business Enablement:* Since the Group uses significant volumes of personal data, Privacy Policy become a prerequisite to building enduring business relationships.
- *Legal Protection:* Appropriate privacy policies offer an opportunity to eliminate allegations of unlawful usage of personal information.

1.2 The policies and guidelines in this Data Privacy Manual (the "**Manual**") are based on the requirements of Republic Act No. 10173, also known as the Data Privacy Act of 2012 ("**DPA**"), its Implementing Rules and Regulation ("**IRR**") and other relevant policies, including issuances of the National Privacy Commission ("**NPC**").

1.3 This Manual shall inform the data subjects of the Group's data protection and security measures, and may serve as the guide for data subjects in exercising their rights under the DPA.

2.0 PURPOSE/OBJECTIVE(S)

2.1. Compliance with laws and regulations

- This Manual defines requirements to help ensure compliance with laws and regulations applicable to the Group's collection, storage, use, transmission, disclosure to third parties, retention, disposal and destruction of personal data. This will also help ensure that applicable regulations and contracts regarding the maintenance of privacy, protection and cross border transfer of personal data are adhered to.

2.2. Better personal data management

- This Manual will help ensure that the Group manages personal data in an accessible and transparent way. This Manual will help limit the use of personal data to identified business purposes for which it is collected.

2.3. Protection against security threats

- This Manual will help ensure that all of the personal data in Group's custody is adequately protected against threats to maintain its security.

2.4. Employee awareness

- This Manual will help create an awareness of privacy requirements to be an integral part of the day-to-day operation of every employee and ensure that all employees understand the importance of privacy practices and their responsibilities for maintaining privacy. This will also help ensure that the Group's employees are fully aware of the contractual, statutory or regulatory implications of any privacy breaches. This will help ensure that all employees are aware of the processes that need to be followed for collection, lawful usage, disclosure or transfer, retention, archival and disposal of personal information.

2.5. Data protection by third parties

- This Manual will help ensure that all third parties collecting, storing and processing personal data on behalf of the Group provide adequate data protection.

3.0 DEFINITION OF TERMS

Access	Refers to an individual's right to see and know about his or her own personal information that the Group holds.
Affiliation	Refers to a corporation that directly or indirectly, through one or more intermediaries, is controlled by, or is under the common control of another corporation.
Aggregate	Refers to presenting information in segments or categories.
Anonymize	Refers to the process of collection of personal data or information such that a natural person cannot be identified on the basis of the output collection of data or information.
Automated decision-making	Refers to a wholly or partially automated processing operation that serves as the sole basis for making decisions that would significantly affect a data subject. It includes the process of profiling based on an individual's economic situation, political or religious beliefs, behavioral or marketing activities, electronic communication data, location data, and financial data, among others.
Automated processing	Refers to the creation and implementation of technology that automatically processes data. This technology includes computers and other communications electronics that can gather, store, manipulate, prepare and distribute data. The purpose of automated data processing is to quickly and efficiently process large amounts of information with minimal human interaction and share it with a select audience.
Collection	Refers to the process of gathering, acquiring or obtaining personal information from any source, by any means, in circumstances where the individual is identified or is reasonably identifiable. It includes information that: • is publicly available information about an identifiable individual that the Group comes across; • information the Group receives directly from the individual; and • information about an individual the Group receives from somebody else.
Compliance Officer for Privacy ("**COP**")	Refers to an individual that performs some of the functions of a DPO, as provided in NPC Advisory No. 17-01.
Contractors	Refer to agents, suppliers, franchisees, concessionaires, guests, lessors, tenants, consignors, and business partners.
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. Consent must be time-bound in relation to the declared, specified, and legitimate purpose. Consent given may be withdrawn.
Cookie	Refers to a block of data that a web server places on a user's personal computer that is typically used to ease navigation through the site. However, it is also a useful means of the website identifying the user, tracking the user's path through the site, and identifying repeat visits to the site by the same user (or same user's machine). This can then lead to a website owner being able to profile an individual user's browsing habits - and all potentially done without the knowledge, or consent, of the user.
Data	Any information being processed using equipment operating automatically in response to instructions given for that purpose and

	that has been recorded with the intention that it should be processed by means of such equipment, or is recorded as part of a relevant filing system, or with the intention that it should form part of a relevant filing system, or information which does not fall within the previous definitions but forms part of an accessible record.
Data Privacy Act ("**DPA**")	Refers to Republic Act No. 10173 or the Philippine Data Privacy Act of 2012, its IRR and any issued and/or subsequent circular memorandum and advisories to be issued by NPC.
Data Privacy Manual ("**Manual**")	Refers to this Data Privacy Manual of the Group which establishes policies, and implements measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights.
Data Protection Officer ("**DPO**")	Individual designated by the Group to be accountable for its compliance with the DPA, its IRR, and other issuances of the NPC: *provided*, that, except where allowed otherwise by Law or the NPC, the individual must be an organic employee of the Group: provided further, that the Group may have more than one DPO.
Data sharing	Disclosure or transfer to a third party of personal data under the control or custody of PIC: provided, that a PIP maybe allowed to make such disclosure or transfer if it is upon the instructions of the PIC concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a PIC to a PIP.
Data sharing agreement	Refers to a contract, joint issuance, or any similar document that contains terms and conditions of a data sharing agreement between two or more parties: *provided*, that only PICs shall be made parties to a data sharing agreement.
Data subject	Individual whose personal, sensitive personal or privileged information is processed. It may refer to employees (regardless of the type of employment or contractual arrangement), agents, suppliers, franchisees, concessionaires, guests, lessors, tenants, consignors, customers, and business partners.
Data subject information request	Refers to any request received by the firm from a data subject or other individual or legal entity who wishes to receive a copy of all the Personal Data related to it or him that the Group is processing about it or him.
Direct marketing	Refers to communication by whatever means of any advertising or marketing material, which is directed to particular individuals, which includes activities that promote the sale, purchase of products or services, or promote charitable fundraising where the individual is approached directly. It includes in-person approaches to people's houses and approaches by mail, e-mail, facsimile and phone. It includes individually targeted approaches by these means where people are encouraged to buy services at a distance (*e.g.*, to buy by phone, mail or website) or to visit retail and service outlets or to donate to a cause by one of these means.
Disclosure	Means rendering personal data accessible, for example by allowing access to personal data either transferring, distributing, or publishing the personal data.
Encryption method	A technique that renders data or information unreadable ensures that it is not altered in transit, and verifies the identity of its sender.
Filing system	Any set of information relating to a natural or juridical person to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by

	reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.
Guest	Refers to all natural individuals who are not employees (regardless of the type of employment or contractual arrangement), agents, suppliers, franchisees, concessionaires, lessors, tenants, consignors, customers, and business partners, who have access to the Group's facilities and websites.
Legitimate interest	A data privacy principle that allows processing of information only if such processing is compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy.
Mobile application	Refers to the computer program or software application designed to run on a mobile device such as smartphone or tablet computer.
National Privacy Commission ("**NPC**")	NPC is an independent body created under the DPA mandated 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.
Outsourcing	A practice of shifting certain job functions or processing activities to an external contracted third party for a significant period instead of handling them in house.
Personal data	Collectively refers to personal information, sensitive personal information, and privileged information.
Personal data breach (or simply "**breach**")	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. It occurs also when an unauthorized party acquires the personal data of a data subject without it being adequately secured or encrypted.
Personal data life cycle	This is composed of collection, usage, access and correction, disclosure and distribution or data sharing, storage and transmission, retention, and disposal and destruction.
Personal data processing system	Refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.
Personal information	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.
Personal Information Controller ("**PIC**")	Natural or juridical person or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing. The term excludes: • A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or • A natural person who processes personal data in connection with his or her personal, family, or household affairs.
Personal Information Processor ("**PIP**")	Any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject.
Privileged information	All forms of data, which, under the rules of court and other pertinent laws, constitute privileged communication.
Privacy impact assessment ("**PIA**")	A process or tool undertaken and used to identify the potential risks of existing personal or sensitive personal information on Group's

	systems, technology, programs, processes, or activities to an individual's privacy.
Privacy notice	A statement made to a data subject that describes how the organization collects, uses, retains and discloses personal data. A Privacy Notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a Privacy Policy.
Privacy policy	An internal statement that governs the Group's handling practices of personal data. It is directed at the users of the personal data. A Privacy Policy instructs employees on the collection and the use of the data, as well as any specific rights the data subjects may have.
Processing	Refers to any operation or set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing maybe performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system.
Profiling	**Any form of automated processing of personal data consisting of the use of personal data, such as an individual's economic situation, political or religious beliefs, behavioral or marketing activities, personal preferences, electronic communication data, location data, and financial data, among others, in order to evaluate, analyze, or predict his or her performance, qualities, and behavior, among others.**
Pseudomize	Refers to the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.
Reasonable	Generally speaking, it relate to decisions or steps to be taken by the Group in particular circumstances (*e.g.*, when collecting, correcting or using and disclosing information) or to expectations of individuals in those circumstances. Determining what is reasonable involves considering the factual circumstances in which a person or organization is acting rather than the individual's or organization's view of what is reasonable or unreasonable.
Required by law	Required by law refers to circumstances where a law (other than the DPA) requires an organization to collect, use or disclose or deny access to, personal information. In certain instances, failing to comply with such a legal requirement may be an offense. Such a law may specifically require an organization to collect, use, disclose or deny access. It may also be a law that gives another body, such as a government agency, a general information gathering power that includes the power to require an organization to disclose information to it.
Security incident (or simply "**incident**")	An event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data.
Sensitive personal information	Personal information: (1) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (2) about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or

	current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) specifically established by an executive order or an act of Congress to be kept classified.
Third party	All external parties – including without limitation contractors, interns, agents, vendors, service providers and partners – who have access to the Group's information assets, information systems or who are pass personal information from them.
Use	Relates to the handling of the personal information within the Group. Examples of uses of information are: • adding information to a database; • forming an opinion based on information collected and noting it on a file; and • including information in a publication.
Unsolicited personal data	Refers to personal data received by the Group where the Group has taken no active steps to collect the information.
Web beacons	Refers to any of a number of techniques used to track who is reading a web page or email, when, and from which computer. They can also be used to see if an email was read or forwarded to someone else, or if a web page was copied to another website.
Website	Refers to a connected group of pages on the World Wide Web regarded as a single entity, usually maintained by one person or organization and devoted to a single topic or several closely related topics.

4.0 SCOPE AND LIMITATIONS

4.1 This Manual is applicable to all business units of the Group, as defined in ***Annex B_ CPGI-DPM-2018 _Business Units Under CPGI***.

4.2 This Manual is applicable to all employees of the Group (regardless of the type of employment or contractual arrangement), and to the extent practicable, agents, suppliers, franchisees, concessionaires, guests, lessors, tenants, consignors, customers, and business partners who may receive personal information from the Group, have access to personal data collected or processed by or on behalf of the Group, or who provide information to the Group.

4.3 This Manual covers the treatment of personal data gathered and used by the Group for lawful business purposes. This Manual also covers the personal data the Group shares with authorized third parties or that third parties share with the Group.

4.4 Any requests for exceptions to this policy should firstly be referred to the Data Protection Officer ("**DPO**"). Written approval from the DPO should then be forwarded to the person requesting the exception.

5.0 DATA PRIVACY PRINCIPLES

All processing of personal data within the Group shall be allowed subject to adherence to the following general principles of privacy:

5.1. TRANSPARENCY

The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data by the Group, including the risks and safeguards involved, the identity of persons and entities involved in processing his or her personal data, 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.

5.2. LEGITIMATE PURPOSE

The processing of personal data by the Group shall be compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy.

5.3. PROPORTIONALITY

The processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. The Group shall process personal data only if the purpose of the processing could not reasonably be fulfilled by other means.

6.0 PROCESSING OF PERSONAL DATA/PERSONAL DATA LIFE CYCLE

6.1. COLLECTION

6.1.1. Collection of personal information

a. The Group must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the Group's functions or activities. The Group may collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
b. Where it is reasonable and practical to do so, the Group will collect personal information about an individual only from the individual alone. If, however, this information is collected from a third party, the Group must act reasonably to ensure the individual is or has been made aware of the matters listed under ***6.1.3 Components of Privacy Notice*** below.

6.1.2. Collection of sensitive personal information

a. The Group must only collect sensitive personal information:
    i. Where the information is reasonably necessary for one or more of the Group's functions or activities and with the individual's explicit consent (Refer to ***Annex O_ CPGI-DPM-2018 _Suggested Wordings for Consent Form Template***);
    ii. if the collection is required by law.

    Should collection of sensitive personal information of an individual be necessary, the Group must take reasonable steps to ensure that the individual is aware of the matters listed under ***6.1.3 Components of Privacy Notice*** below.

6.1.3. Components of Privacy Notice

Whenever the Group collects personal data about an individual, the Group must take reasonable steps to ensure that the individual is aware of the following as may be applicable:

a. *Service description*
    - The Group shall provide an overview of the service(s) within scope of a notification. It is important for data subjects to understand the nature of a service and the processing of the personal information collected, so that they can provide consent that is voluntary, specific and informed. For brevity of the notice, a meaningful name or short phrase for each service may be used but it should be possible (*e.g.*, via a hyperlink) to associate that name or phrase with an overview of the service sufficient for data subjects to provide voluntary, specific and informed consent.
b. *Identification of the Group*
    - The Group shall ensure that the identity and contact details of the Group as the organization collecting and storing the information are provided, accessible or made accessible to data subjects. The contact information and/or address of the Data Privacy Officer ("**DPO**") of the Group or other person/s-in-charge of privacy

practices and responsible for privacy concerns must be provided, accessible or made accessible to data subjects.

c. *Personal data that are collected*
   - The Group shall provide data that allows data subjects to understand what personal data attributes are to be collected even where the collection of the particular personal data attributes is appears to be obvious. The Group shall also specify which personal data attributes are mandatory for provision of the service(s) and shall present the actual personal data attributes to be collected, where feasible, before collection.

d. *Collection method*
   - The Group shall inform the data subject the collection methods of personal data attributes. The Group shall provide clear explanations of all (obvious or non-obvious) personal data collection methods (direct or indirect).

e. *Timing of collection*
   - The Group shall give notice about when personal data will be collected, including where personal data is intended to be collected long after the notification to data subject.

f. *Purposes for which the personal data will be collected and used*
   - The Group shall specify the purpose of collection of personal data and shall explain how it will be used in a manner that allows the data subject to clearly and readily understand the purpose. If the purpose of the use varies among the personal data attributes being collected, the Group shall clearly mark which purpose applies to which personal data attribute.
   - The Group shall provide the purpose for each personal data attribute in the notice.
   - The Group shall order the presentation of personal data uses in its notices according to its general assessment of impact to the corresponding population of data subjects, highest impact first.

g. *Storage and transmission of the personal data*
   - The Group should specify the data protection measures on storage, transmission and reception of the personal data.

h. *Method of use*
   - The Group should provide notification to the data subject whether the personal data will be used as is, or if the personal data will be subject to additional processing before being used for the stated purposes. If the Group intends to process the personal information in some way prior to using it for the stated purposes, the Group shall provide relevant information to the data subject as to that the said processing.

i. *Location of personal data*
   - The Group shall specify the location where personal data will be stored and processed. If multiple locations are involved, each location shall be specified.

j. *Third party transfer*
   - The Group shall give notice to data subjects on whether or not personal data will be transferred to a third party.
   - If the Group transfers personal data to a third party, it shall notify the data subject of recipient of such personal data. Although the Group needs to identify and give notice of individual third party recipients, the Group may specify a group of recipients using clearly defined criteria where appropriate.
   - If the Group transfers personal data to a third party, it shall notify the data subject of the purpose(s) for which the personal data is being transferred.

k. *Retention*
   - The Group should specify the period for which personal data shall be retained as per identified business purpose or as mandated by regulations, whichever is later, and/or the de-identification schedule of all personal data. The Group should specify the data protection measures on disposal of the personal data.

For the policy on the retention policy, please refer to Appendix F_ CPGI-DPM-2018 _Records Retention Policy.

l. *Participation and rights of data subject*
- The Group shall notify data subjects of their right to access their personal data possessed and/or controlled by the Group, as well as their rights for the correction of personal data. The Group shall give notice of the following aspects of that access:
  i. what personal data attributes the data subject can request access to and the means by which the data subject can make such a request;
  ii. what information will be required from the data subject in order to authenticate themselves to an acceptable level of assurance, prior to authorizing access to any personal data (to avoid the risk of inappropriate disclosure);
  iii. the timelines within which a request will be acted upon;
  iv. any fees which may be charged for such access, where the charging of such fees is permitted;
  v. the means by which a data subject can challenge the accuracy and completeness of the personal data and have it amended as appropriate; and
  vi. where correction of personal data is not possible (*e.g.*, investigation files), the Group shall explain the reason for refusing to correct the information to the data subject.
- The Group shall indicate the following rights of data subject:
  i. *Right to access and correction.* The Group shall include the fact that the data subject may access the information and seek correction.
  ii. *Right to complaint.* The fact that he or she may make a privacy complaint and how the Group will act on such complaint;
  iii. *Right to inquiry.* The Group shall provide the contact information for inquiries regarding the processing of personal information.

m. *Intended recipients of personal data*
- The Group shall include the intended recipients or entities to which the Group usually discloses information of that kind, including any overseas recipients and the countries in which those recipients are likely to be located.

n. *Legal basis of collection*
- Any law that requires the particular information to be collected;

o. *Main consequences of not providing personal data*
- The main consequences (if any) for the individual if all or part of the information is not provided and of withholding or withdrawing consent to the collection, use and disclosure of personal data for identified purposes should also be disclosed.

Refer to the following for the templates on suggested wordings for Consent Form and Privacy Policies:
Annex H_ CPGI-DPM-2018 CCTV Surveillance Privacy Policy
Annex O_ CPGI-DPM-2018 _Suggested Wordings for Consent Form Template
Annex P_ CPGI-DPM-2018 Privacy Policy for Website

6.1.4. Consent

a. In circumstances where consent is needed, the Group shall obtain the explicit consent of the data subject as evidenced by any of the following modes: written, electronic or recorded means, subject to the rules on authentication provided under existing laws and regulations (*e.g.*, the DPA, the Rules of Court and the Rules on Electronic Evidence).
b. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose.

c. When necessary, provide the data subject a mechanism through which they can subsequently rescind the permission(s) earlier provided and opt-out.

Refer to the following for the templates on suggested wordings for Consent Form, refer to ***Annex O_ CPGI-DPM-2018 _Suggested Wordings for Consent Form Template.***

6.1.5. Receiving unsolicited personal data

Where employees and authorized contractors receive unsolicited personal data about an individual, they must determine within a reasonable time whether they could have collected the information in accordance with sections ***6.1.1 Collection of personal information, 6.1.2 Collection of sensitive personal information, 6.1.3 Components of Privacy Notice and 6.1.4 Consent***. Should the collection not be in accordance with the said sections, the employees and authorized contractors, to the extent allowed by law and to the extent reasonable and practicable, must either destroy or de-identify the personal data.

6.1.6. Collection of personal data for research

a. Employees and authorized contractors may collect the personal data of an individual for research from a party or parties other than the data subject when:
   - The personal data is publicly available; or
   - Have the consent of the data subject for purpose of research.

b. To the extent applicable and reasonable, information about a data subject is aggregated and anonymized such that data subject is never identified as an individual.

c. Adequate safeguards are in place and no decision directly affecting the data subject shall be made on the basis of the data collected or processed.

6.1.7. Collection of personal data for CCTV surveillance

a. Some of the Group's areas, buildings and sites use CCTV systems to monitor their exterior and interior 24 hours a day for security reasons. This data is recorded. Use of CCTV and recording of CCTV data is only carried in accordance with the Group's approved guidelines.

b. The Group shall take reasonable efforts to alert the individual that the area is under electronic surveillance (i.e., posting of Privacy Notices on conspicuous areas).

For the Privacy Policy for camera surveillance, refer to ***Annex H_ CPGI-DPM-2018 CCTV Surveillance Privacy Policy*** **Collection of personal data through websites**

a. The Group's website that does any of the following should have a Privacy Notice:
   - Collects personal data (*e.g.*, guests filling in web forms, feedback forms, applications for employment, shopping online, posting of product reviews, and so on),
   - Uses cookies and/or web beacons, and
   - Covertly collects personal data (*e.g.*, IP addresses, e-mail addresses, and so on).

b. Websites, if performing any of the items mention in (a) above, shall obtain the website guest's prior permission and providing the website guest with access to information about and where the data will be used. The websites shall comply with sections ***6.1.1 Collection of personal information, 6.1.2 Collection of sensitive personal information, and 6.1.4 Consent*** of this Manual.

c. The Privacy Notice shall disclose the personal data collected, including the use of website cookies and/or web beacons, and shall comply with the provisions in ***6.1.3 Components of Privacy Notice*** and establish a cookie policy when needed.

d. The Privacy Notice shall be placed in a reasonably obvious position on the homepage (in the sub navigation menu which is normally situated in a bottom

position on the homepage, and should be separate from the Terms and Conditions document).

e. The Privacy Notice shall be placed on pages where personal data is collected or, if the website uses cookies and/or web beacons, this could effectively mean, on all pages.

For the Privacy Policy for websites, refer to ***Annex P_ CPGI-DPM-2018 Privacy Policy for Website.***

6.2. USAGE

6.2.1. Personal data must be processed fairly and lawfully, and adequate and not excessive in relation to the purposes for which they are collected and processed. Personal information must be accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

6.2.2. As a general rule, the Group's management and employees must not use personal data about an data subject other than for its primary purpose of collection, unless:

a. The data subject has consented to the use or disclosure; or
b. The data subject would reasonably expect the Group to use or disclose non-sensitive information for a secondary purpose and the secondary purpose is related to the primary purpose; or
c. The Group has reason to suspect that unlawful activity has been, or may be engaged in, and uses or discloses the personal information as required by applicable laws and regulations or as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
d. The use or disclosure is required or authorized by or under law; or
e. The Group reasonably believes that the use or disclosure is reasonably necessary for a specified purpose by or on behalf of an enforcement body; or
f. The Group reasonably believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to public health or public safety or the life or health of an data subject; or
g. Management and employees must only use or disclose personal information in a manner consistent with any Privacy Notice provided to the data subject.

6.2.3. Direct Marketing

a. When contacting data subjects for direct marketing in whatever form, the following conditions must be present:
   - The Group provides simple means by which the data subject may easily request not to receive direct marketing communications from the Group;
   - In each direct marketing communication with the data subject, the Group draws to the attention of the data subject, or prominently displays a notice, that he or she may express a wish to "unsubscribe" or "opt-out" or not to receive any further direct marketing communications;
   - The data subject has not made a request to the Group not to receive direct marketing communications;
   - The Group will not charge the data subject for giving effect to a request not to receive direct marketing communications.
b. *Personal Information for Direct Marketing.* Use of personal information for direct marketing purposes is permitted where:
   - The information has been collected from the data subject and the data subject would reasonably expect the Group to use it for that purpose; or
   - The information has been collected from a party other than the data subject and the Group has either obtained the consent of the data subject.

c. *Sensitive Personal Information for Direct Marketing.* Use of sensitive personal information for direct marketing is permitted only when the data subject has consented the use or disclosure of the information for that purpose.

6.2.4. Use of Government-Related Identifiers

The Group must not use and disclose government-related identifiers unless such usage is reasonably necessary for the Group to verify the identity of the individual for the purpose of the Group's activities, or alternatively, the use is required or authorized under law.

6.3. ACCESS AND CORRECTION

6.3.1 As a general rule, the DPO shall, at the request of the data subject, provide the data subject with access to his/her personal data within a reasonable time after such request is made and will consider a request from the data subject for correction of that information.

6.3.2 The DPO can only impose a minimal and reasonable charge upon the data subject to cover the cost of locating, retrieving, reviewing and copying any material requested by the data subject.

6.3.3 The DPO may, however, choose not to provide the data subject with access to such information. This would include cases where:

a. The Group reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
b. Providing access would have an unreasonable impact on the privacy and affairs of other individuals;
c. The request for access is frivolous or vexatious or the information requested is trivial;
d. The information relates to anticipated or existing legal proceedings and would not be discoverable in those proceedings;
e. Providing access would reveal the intentions of the Group in relation to negotiations with the said data subject in such a way as to prejudice those negotiations;
f. Providing access would be unlawful;
g. Denying access is authorized under law or a court/tribunal order;
h. Providing access would be likely to prejudice an investigation of possible unlawful activity or security, defense or international relations; or
i. Providing access would be likely to prejudice activities which are carried out by the Group on behalf of an enforcement body; or
j. Where the data subject:
   - has been refused access to his/her personal data which the Group holds about him/her; and/or
   - having requested correction of his/her personal information, is refused.

   In such cases, the DPO will give the data subject a written notice that sets out:
   - The reasons for the refusal where it is reasonable to do so; and
   - The way in which the data subject may make a complaint about such refusal.

For the templates used for allowing data subject:

- ***Annex A_ CPGI-DPM-2018 _Access Request Form***
- ***Annex C_ CPGI-DPM-2018 _Inquiry_Complaints_Access and Deletion Request summary Report***
- ***Annex E_ CPGI-DPM-2018 _Request For Correction and Deletion Form***

6.4. DISCLOSURE AND DISTRIBUTION/DATA SHARING TO THIRD PARTIES

6.4.1. Personal data shall be disclosed to third parties only for identified lawful business purposes and after obtaining appropriate consent from the data subjects, unless a law or regulation allows or requires otherwise.

Where reasonably possible, management shall ensure that third parties collecting, storing or processing personal data on behalf of the Group have:

a. Signed agreements to protect personal data consistent with this Manual, Privacy Notices and information security practices or implemented measures as prescribed by law;
b. Signed non-disclosure agreements or confidentiality agreements which include privacy clauses in the contracts;
c. Established procedures to meet the terms of their agreement with the Group to protect the personal information; and
d. Remedial action to be taken in response to the misuse or unauthorized disclosure of personal information by a third party collecting, storing or processing personal information on behalf of the Group.

For the suggested wordings, please refer to:

- ***Annex K_ CPGI-DPM-2018 _Data Sharing Agreement within CPGI Template***
- *Error! Reference source not found.*
- *Error! Reference source not found.*

6.4.2. Cross-border Data Flows

a. Any form of sharing personal data to an entity or individual outside the Philippines should be allowed only if:
   - The data subject has consented to the transfer; or
   - The Group reasonably believes that the recipient is subject to laws or a contract enforcing information handling principles substantially similar to applicable privacy laws in the Philippines (*i.e.*, DPA); or
   - The transfer is necessary for the performance of a contract between the individual and the entity; or
   - The transfer is necessary as part of a contract in the interest of the data subject between the Group and a third party; or
   - The transfer is for the benefit of the data subject; or
   - It is impractical to obtain the consent of the data subject; or
   - To the extent practicable, the data subject would likely consent.

b. The Group should take reasonable steps so that the information transferred will be held, used and disclosed consistently with the applicable privacy laws in the Philippines (*i.e.*, DPA).

6.5. STORAGE AND TRANSMISSION

The Group shall ensure that appropriate physical, technical and organizational security measures are implemented on personal information storage facilities.

6.6. RETENTION

6.6.1 Personal data shall be retained only for the duration necessary to fulfill the identified lawful business purpose. All personal data of the data subjects shall be retained only for as long as necessary:

a. for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
b. or the establishment, exercise or defense of legal claims;

c. for legitimate business purposes, which must be consistent with standards followed by the industry; or
d. in some specific cases, as prescribed by law.

6.6.2 Guidelines and procedures shall be developed for the retention of personal data. These shall address minimum and maximum retention periods, and modes of storage.

6.6.3 Personal data collected for other purposes may be processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods, provided that adequate safeguards are guaranteed by said laws authorizing their processing.

6.6.4 Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

6.7. DISPOSAL AND DESTRUCTION

6.7.1 Guidelines and procedures shall be developed for the secure disposal and destruction of personal data to prevent further processing, unauthorized access, or disclosure to any other party or public, or prejudice the interests of the data subjects. These should address the category of risk ratings assigned for the personal data. These shall also address disposal process on, but shall not be limited to, the following types of storage:
a. files that contain personal data, whether such files are stored on paper, film, optical or magnetic media;
b. computer equipment, such as disk servers, desktop computers and mobile phones at end-of-life, especially storage media, provided that the procedure shall include the use of degaussers, erasers, and physical destruction devices, among others; and
c. offsite storage or archives.

6.7.2 Upon the expiration of identified lawful business purposes or withdrawal of consent, the Group must take reasonable steps to securely destroy or permanently de-identify or anonymize personal information if it is no longer needed. Data may be anonymized, or pseudonyms used, as deemed appropriate and as may be applicable, to prevent unique identification of an individual.

6.7.3 Disposal should be in a manner that the personal data should be unreadable (for paper) or irretrievable (for digital records).

7.0 SECURITY MEASURES

Security measures aim to maintain the availability, integrity and confidentiality of personal data and protect such 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. The following gives a general description of those measures.

7.1. ORGANIZATIONAL MEASURES

The Group considers the following measures for data protection:

7.1.1 Compliance Monitoring and Reporting

a. To ensure compliance with the DPA and the NPC, the Group shall undertake the necessary steps as follows:
   i. Compliance with NPC registration requirements:
      - Appointment and registration of a DPO and of Compliance Officers for Privacy ("**COP**") for each of the legal entities mentioned in ***Annex***

B_CPGI_DPM_2018 Business Units under CPGI, and the update and/or renewal of such registration;

- Registration of personal data processing systems and continuous registration of new personal data processing systems, and the update and/or renewal of such registration;
- Registration of automated processing systems and continuous registration of new automated processing systems, and the update and/or renewal of such registration.

ii. Establishment of a Data Privacy Committee, its composition and specific roles to assist in compliance and implementation of the guidelines in this Manual, the DPA, its IRR and applicable laws and regulations. Refer to ***section 7.1.2 Data Privacy Office/Data Privacy Committee*** below.

iii. Establishment of a Data Privacy Manual, which includes guidelines for the annual review and update thereof. Refer to ***section 7.1.6 Review of Data Privacy Manual*** below.

iv. Establishment of a Privacy Management Program, which includes implementation plan of data privacy and protection controls.

v. Conduct of a Privacy Impact Assessment ("**PIA**") for manual and electronic systems that process personal data. Refer to ***section 7.1.3 Conduct PIA*** below.

vi. Conduct of training and awareness seminars to promote entity-wide compliance to applicable laws and regulations. Refer to ***section 7.1.4 Trainings/Seminars and Certifications*** below.

b. Record and/or document activities carried out by the DPO to ensure compliance with DPA, its IRR and other relevant policies.

c. Non-compliance with this Manual may result in a breach of the Data Privacy Policy, the DPA and other applicable laws. Instances of noncompliance with privacy policies and procedures shall be documented and reported and, if needed, corrective and disciplinary measures shall be taken on a timely basis.

7.1.2 Data Privacy Committee

The Group recognizes the need to define governance for the data privacy initiatives. Responsibility and accountability shall be assigned to a group of qualified individuals (known as *Data Privacy Committee*) for developing, documenting, implementing, enforcing, monitoring and updating the Group's Manual.

For a more detailed discussion for structure and the roles and responsibilities of the Data Privacy Committee, refer to:

- ***Appendix A_ CPGI-DPM-2018 _Data Privacy Committee Structure***
- ***Appendix B_ CPGI-DPM-2018_ Data Privacy Roles and Responsibility***

For a detailed qualifications of the Data Privacy Office, refer to ***Annex J_ CPGI-DPM-2018 _DPO and COP qualifications.***

7.1.3 Conduct PIA

a. The organization shall conduct a PIA relative to all activities, projects and systems involving the processing of personal data. It may choose to outsource the conduct of PIA to a third party.
   For the guidelines and suggested templates in conducting PIA, refer to the following:
   - ***Appendix C_ CPGI-DPM-2018_ Guidelines for PIA***
   - ***Annex F_ CPGI-DPM-2018 _Privacy Impact Assessment Tracker***
   - ***Annex G_ CPGI-DPM-2018 _Privacy Impact Assessment Template***

b. In the conduct of PIA, personal data flow diagrams may be prepared to support the assessment made. These personal data flow diagrams should be regularly updated, as needed, or at least annually.

c. In the conduct of PIA, prepare and consolidate the personal data processing systems (whether automated or manual) in compliance with the legal and regulatory requirements of the NPC. These personal data processing systems should be regularly updated, as needed, or at least annually.

For the personal data processing systems template, refer to ***Annex Q_ CPGI-DPM-2018 Data Processing System Template***

The PIA shall include the preparation of documents inventory. The Group shall compile a list of documents (including forms) that are required to support the Group's various business processes and that which process significant amount of personal data. With this document inventory, the Group's objective is to get a clear view of its significant documents collecting personal data that are to be protected.

Second, the Group must assess each document in terms of its confidentiality and sensitivity. This is done so that the appropriate level of security protection can be assigned to the document. Each document has to be classified according to a predetermined document classification scheme of the Group.

Third, it is important for the Group to have clearly determine which departments and/or employees within the Group are responsible for handling the document at each stage of the life cycle and business process. Therefore, the Group must construct a document flow diagram. This traces the movement of the document through its life cycle based on the Group's business processes.

For the significant personal data document inventory te`mplate, refer to ***Annex Q_ CPGI-DPM-2018 _Inventory of Data Processing System Template***

e. The Group shall also perform an onsite audit to assess the adequacy of existing PIA, data flow diagrams, personal data processing systems inventory and personal data document inventory. It must then address identified weaknesses and vulnerabilities to minimize the Group's risk exposures. It must also ensure or check that candidates for PIA and those undergoing PIA were properly identified and tracked.

7.1.4 Trainings/Seminars and Certifications

a. The Group shall conduct trainings or seminars on data privacy and security at least once a year to keep its employees and personnel generally aware of personal data privacy and protection and to make them familiar with the Group's policies and practices for compliance with the law.
b. For training to be effective, it should:
   - Be given to new employees and should be conducted periodically after their employment,
   - Cover the policies and procedures established by the Group,
   - Be delivered in an appropriate and effective manner, and
   - Circulate essential information to relevant employees as soon as practical or if an urgent need arises.
c. The Group shall ensure the attendance and participation of employees in relevant trainings and orientations, as often as necessary.
d. The Group shall support certifications on data privacy and security, whenever necessary.

For the data privacy orientation materials, refer to ***Annex N_ CPGI-DPM-2018 _Data Privacy Awareness Training***

7.1.5 Duty of confidentiality

a. All employees and authorized representatives of contractors in the name of the Group shall be required to sign a Non-Disclosure Agreement which fully details their duty of confidentiality as regards to the personal data to which they are exposed to and as regards the personal data are shared to them, in the case of third-parties, in the performance of their specific job functions.
b. All employees and authorized representatives of contractors of the Group who have access to personal data shall:
   - Operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.
   - Not make use of personal data, except for the purpose required by their specific job functions.
   - Not share personal data to any person or entity, except as allowed by data sharing agreements or applicable laws.
   - Take such steps as are reasonable to preserve the confidentiality of personal data.
   - Not reproduce personal data, except to the extent required by their specific job functions.
c. Security clearances should be issued to persons exposed to the processing of personal data.
d. The employees' and authorized representatives of contractors' duty of confidentiality remains as a continuing obligation to the Group for an indefinite period and extends beyond any termination of their employment period or contract.
e. The Group reserves the right to take disciplinary action, up to and including termination for violations of the Non-Disclosure Agreement.

7.1.5 Review of Data Privacy Manual

a. This Manual shall be reviewed at least annually, or earlier if deemed required, to check compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts, and must be documented.
b. For this purpose, the DPO shall lead the review and/or revision of policies detailed in this Manual. In addition, the Legal Department shall review any conflict between the Policy/Guidelines and any local law, and make recommendations to Senior Management and Board of Directors, as necessary, who shall review and approve this Manual at least on an annual basis.

7.2. PHYSICAL SECURITY MEASURES

The Group recognizes the need to implement security measures to monitor and limit access to the facility containing the personal data, including the activities therein. As such, the following physical security measures shall provide for the actual design of the facility, the physical arrangement of equipment and furniture, the permissible modes of transfer, and the schedule and means of retention and disposal of data, among others. The following measures will also help ensure that mechanical destruction, tampering and alteration of personal data under the custody of the organization are protected from man-made disasters, power disturbances, external access, and other similar threats.

7.2.1 Role of Data Privacy Committee

a. The DPO, in coordination with the Data Privacy Committee, Administration Department and Distribution Centers, shall develop and implement policies and procedures for the Group to monitor and limit access to, and activities in, the building property of the Group, including the branches', subsidiaries' and affiliates' offices, warehouse facilities, areas and workstations where personal data are collected, used, stored and disposed.

b. The DPO, in coordination with Data Privacy Committee, shall also develop and implement policies in using IT assets as well as policies in using social media and mobile devices, if to be allowed.

7.2.2 Role of employees and contractors

All employees and contractors must follow policies and procedures developed and implemented by the DPO.

7.2.3 Minimum physical security policies and procedures

a. Format of personal data to be collected

i. Personal data collected may be in electronic or physical format. Only those systems, websites, mobile applications, and paper forms allowed and acknowledged by the Group should be used to collect personal data.

b. Storage type and location

i. All personal data stored by the Group shall be placed in storage rooms with limited access only to selected individuals for paper-based forms and in filing cabinets with locks for constantly used paper-based forms, and secured server and database rooms in a controlled environment for electronic format.

c. Access procedure of personnel

i. The Group should strictly regulate access to personal data under its control. Approved access should be granted only to authorized personnel.
ii. Authorization should be governed by strict procedures contained in the Group's policies and procedures, and formal contracts signed by the employees, contractors, and third parties.
iii. Review of the appropriateness of the access of the authorized personnel must be part of the policies and procedures.

d. Monitoring and limitation of access to room or facility

i. Only authorized employees, personnel or persons should be allowed inside the storage area, distribution center and data center. Borrowing of identification cards and room keys should not be allowed, unless the requesting employee or visitor will be accompanied by the authorized personnel.
ii. Only persons issued with security clearances should have access to the Group's rooms and facilities storing personal data, unless required by law or exception is duly approved by appropriate management.
iii. The Group should maintain a log, from which it can be ascertained which room or facility is accessed, including when, where, and by whom. The Group should regularly review the log records, including applicable procedures.
iv. A CCTV record must be maintained for security purposes and privacy notice for the use of such camera surveillance should be posted in conspicuous areas of the building/facility.

*For more details, refer to the section on **Collection of personal data for CCTV surveillance under 6.1.3 Components of Privacy Notice.***

e. Design of office space/ work station

i. Positioning of office space or workstation is encouraged to be arranged with considerable spaces between them to maintain privacy and protect the processing of personal data. Employees and agents should avoid shoulder surfing, eavesdropping and other unauthorized access.

f. Persons involved in processing, and their duties and responsibilities

i. Persons involved in processing shall always maintain confidentiality and integrity of personal data.

ii. They are not allowed to bring their own gadgets or storage device of any form, unless allowed and approved by appropriate management under certain/special circumstances, when entering the data storage room.

g. Modes of transfer of personal data within the Group, or to third parties

i. Transfer of personal data within the Group or to third parties is considered part of the purpose for which personal data was originally collected.
ii. The DPO, in coordination with the Data Privacy Committee, should have policies and procedures regarding secure transfer of personal data within the Group. Policies and procedures should have security measures set forth in the DPA and other related issuances.
iii. A contract, including confidentiality clause and outsourcing/data sharing agreement, as deemed necessary, should be made for transferring of personal data within the Group and to third parties. Contracts and agreements with business units within the Group and with third parties should aim for data privacy compliance as set forth in the DPA, other related issuances and relevant laws and regulations.

h. Retention and disposal procedure

All personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any party or the public, or prejudice the interests of the data subjects. At the minimum, procedures must be established regarding:

i. disposal of files that contain personal data, whether such files are stored on paper, electronic media;
ii. secure disposal of computer equipment, such as disk servers, desktop computers and mobile phones at end-of-life, especially storage media: provided, that the procedure shall include the use of degaussers, erasers, and physical destruction devises; and
iii. disposal of personal data stored offsite.

7.3. TECHNICAL SECURITY MEASURES

The Group recognizes the need to 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. These security measures include the following, among others:

7.3.1 Role of Data Privacy Office

The DPO, in coordination with the Data Privacy Committee and Information Systems Department, shall continuously develop and evaluate the Corporation's security policies and procedures from collection, usage, sharing, storage and disposal of Personal Data.

7.3.2 Role of employees and contractors

All employees and authorized contractors must follow policies and procedures developed and implemented by the DPO.

7.3.3 Minimum technical security policies and procedures

a. Access controls

The Group shall establish logical access control policy and procedures to limit access to systems processing personal information only to authorize personnel based upon assigned roles and responsibilities.

b. Monitoring for security incidents and personal data breaches

The Group shall use systems (*e.g.*, intrusion detection system) to monitor security breaches and alert the Group of any attempt to interrupt or disturb the system. When deemed appropriate, conduct also personal data breach exercises.

c. Security features of the software/s and application/s used
The Group shall first review, evaluate and integrate privacy concepts on software applications before the installation thereof in computers and devices of the organization to ensure the compatibility of security features with overall operations.

d. Process for regular testing, assessment and evaluation of effectiveness of security measures
The Group shall review security policies, conduct vulnerability assessments and perform penetration testing within the Group on regular schedule to be prescribed by the appropriate department or business unit.

e. Backup, restoration and recovery of personal data
The Group shall maintain a backup file for all personal data within its possession for recovery and restoration purposes in cases of data breach or security incidents.

f. Network security
The Group shall deploy security measures on a network level to protect its underlying network infrastructure from unauthorized access, disclosure, erasure, and modification of personal data.

g. Encryption, authentication process, and other technical security measures that control and limit access to personal data
Controls shall be implemented to desktops, mobile devices, servers, and other devices used for accessing, processing, transmitting, and storing personal data to protect against possible data breaches

At the minimum, the controls for the following should be established:

i. Patch management procedures
ii. Anti-virus and Malware protection
iii. Encryption
iv. Online access to personal data
v. Emails
vi. Portable media
vii. Identity access management
viii. Software development and change management procedures
ix. Host security controls

8.0 SECURITY INCIDENT AND BREACH RESPONSE AND NOTIFICATION

8.1. Creation of a Data Breach Response ("DBR") Team

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

A DBR Team must be created, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach. The Team should consist of the following members:

a. *Help Desk Personnel* – The 'one point contact' for all the users for all security incidents. He or she should try and obtain as much information as possible from the person reporting the security incident. Help Desk is responsible for evaluating the impact and

urgency of the security incident and appropriately initiating the escalation process. He or she is also responsible for logging, tracking, and maintaining history record or related problem documentations through the Group's ticketing system and problem and incident management protocols.

For the template of monitoring the activities for the investigation and/or resolution of security incidents, refer to ***Annex I_ CPGI-DPM-2018 _Data Breach Incident Report Form.*** *Head of Security Department* – Security Department should be the Team Leaders for all physical security-related security incidents including the:

- Diagnosis of the cause of incident,
- Determination of solution required to restore service,
- Resolution of security incidents, and
- Escalation of unresolved security incidents to the appropriate person or level.

b. *Head of IT* – IT should be the Team Leaders for all Information Technology-related security incidents including the:

- Diagnosis of the cause of incident,
- Determination of the solution required to restore service,
- Resolution of security incidents, and
- Escalation of unresolved security incidents to the appropriate person or level.

c. *Head of Legal Department* – Legal Department should be responsible for providing legal advice on the management of security incidents reported.

d. *Head of Human Resource ("HR")* – HR should be responsible for imposing disciplinary action to be taken and/or made to the employee involved.

e. *Head of Internal Controls and Compliance* – Internal Controls and Compliance should be responsible for validating that actions taken are aligned with the established policies and procedures and existing laws and regulations, particularly on data privacy.

8.2. Measures to prevent and minimize occurrence of security incidents and personal data breach

Implementation of organizational, physical and technical security measures is important to assure the timely discovery of a security incident and prevent or minimize the occurrence of a personal data breach. Such safeguards may include:

- Conducting PIA to identify attendant risks in the processing of personal data *(Refer to* ***Appendix C_ CPGI-DPM-2018 _Guidelines for PIA****)*
- Implementation of appropriate security measures that protect the availability, integrity and confidentiality of personal data being processed,
- Monitoring of security incidents and personal data breaches and vulnerability scanning of computer networks,
- Attending trainings and seminars for capacity building, and
- Periodical review of policies and procedures being implemented in the Group.

8.3. Procedure for recovery and restoration of personal data

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

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

The DBR Team shall prepare a detailed documentation of every security incident and personal data breach encountered, as well as an annual report, to be submitted to the Management and the NPC, as required by existing laws and regulations, within the prescribed period. *For detailed guidelines, refer to* ***Appendix D: Guidelines for Security Incident Response and Breach Notification****. Refer also to the following templates:*

- ***Annex xx-CPGI-DPM-YEAR Data Breach Incident Report Form Template***
- ***Annex xx-CPGI-DPM-YEAR Data Breach Incident Summary Report*** Notification protocol

The DBR Team shall inform the Management of the need to notify the NPC and the data subjects affected, as necessary based on existing laws and regulations, by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the head of the DBR Team. *For detailed guidelines, refer to* ***Appendix D: Guidelines for Security Incident Response and Breach Notification****. Refer also to the following templates:*

- ***Annex I_ CPGI-DPM-2018 _Data Breach Incident Report Form***
- ***Appendix D_ CPGI-DPM-2018 _Guidelines for Security Incident Response and Personal Data Breach Notification***

9.0 INQUIRIES AND COMPLAINTS

9.1 The DPO and/or the Data Privacy Office of the Group should receive all inquiries and complaints related to the privacy of the data subject as well as entertain and institute an investigation in relation thereof.

9.2 Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the Group, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the Group at webmaster@century-properties.com and briefly discuss the inquiry, together with their contact details for reference.

9.3 Complaints shall be filed in three (3) copies, or sent to webmaster@century-properties.com

9.4 The concerned department or business unit shall confirm with the inquiring party/complainant its receipt of the inquiry/complaint. The COP of the concerned department of business unit shall forward the complaint to DPO of the Group.

For the complete guidelines and templates used, refer to the following:

- ***Appendix E_ CPGI-DPM-2018 _Guidelines in filing a complaint***
- ***Annex C_ CPGI-DPM-2018 _Inquiry_Complaints_Access and Deletion Request summary Report***
- ***Annex D_ CPGI-DPM-2018 _Inquiry and Complaint Form***

10.0 REFERENCES

10.1. APPLICABLE PRIVACY LAW

10.1.1 The Philippine DPA was enacted to:

- protect the privacy of individuals while ensuring the free flow of information to promote innovation and growth;
- regulate the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure and destruction of personal data; and
- ensure that the Philippines complies with international standards set for data protection through the NPC.

10.1.2 This covers the IRR of DPA with respect to data protection, issuances, circular memorandum, advisories and toolkits by the NPC, and other applicable laws and policies in the Philippines and in other jurisdictions as appropriate (***e.g.***, European Union's Regulation 2016/679, also known as General Data Protection Regulation or EU GDPR).

11.0 APPENDICES

Appendix A_ CPGI-DPM-2018 _Data Privacy Committee Structure

Appendix B_ CPGI-DPM-2018 _Data Privacy Roles and Responsibility

Appendix C_ CPGI-DPM-2018 _Guidelines for PIA

Appendix D_ CPGI-DPM-2018 _Guidelines for Security Incident Response and Personal Data Breach Notification

Appendix E_ CPGI-DPM-2018 _Guidelines in filing a complaint

Appendix F_ CPGI-DPM-2018 _Records Retention Policy

12.0 ANNEXES

Annex A_ CPGI-DPM-2018 _Access Request Form
Annex B_ CPGI-DPM-2018 _Business Units Under CPGI
Annex C_ CPGI-DPM-2018 _Inquiry Complaints Access and Deletion Request summary Report
Annex D_ CPGI-DPM-2018 _Inquiry and Complaint Form
Annex E_ CPGI-DPM-2018 _Request For Correction and Deletion Form
Annex F_ CPGI-DPM-2018 _Privacy Impact Assessment Tracker
Annex G_ CPGI-DPM-2018 _Privacy Impact Assessment Template
Annex H_ CPGI-DPM-2018 CCTV Surveillance Privacy Policy
Annex I_ CPGI-DPM-2018 _Data Breach Incident Report Form
Annex J_ CPGI-DPM-2018 _DPO and COP qualifications
Annex K_ CPGI-DPM-2018 _Data Sharing Agreement within CPGI Template
Annex L_ CPGI-DPM-2018 _Data Sharing Agreement with Third-Parties Template
Annex M_ CPGI-DPM-2018 _Outsourcing Sub-contracting Agreement Template
Annex N_ CPGI-DPM-2018 _Data Privacy Awareness Training
Annex O_ CPGI-DPM-2018 _Suggested Wordings for Consent Form Template
Annex P_ CPGI-DPM-2018 Privacy Policy for Website
Annex Q_ CPGI-DPM-2018 _Inventory of Data Processing System Template

Prepared by:	Reviewed by:	Endorsed by:	Approved by:
Daniel S. Dela Cruz	Atty. Isabelita C. Sales	Atty. Isabelita C. Sales	Board of Directors of CPGI

13.0 REVISION HISTORY

Version No.	Last Modified Date	Modified by	Description of Change
000	**08/05/2019**	DPO	Original Draft

14.0 REVIEWING DEPARTMENTS

Department / Division	Name of Signatory	Designation	Signature	Date of Review