PRIVACY OPERATING GUIDELINE
Netsec Technologies Inc.

1.0 PURPOSE AND APPLICATION

Netsec Technologies Inc. (Netsec) endeavors to meet standards and regulations for data protection and privacy. Netsec 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.

This Privacy Operating Guideline (Guideline) serves as the manual to help execute 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").

This applies to Netsec, its employees, Board of Directors, and subsidiary, and to the extent applicable, agents, suppliers, guests, customers, and business partners who may receive personal information from Netsec, have access to personal data collected or processed by or on behalf of Netsec, or who will provide information to Netsec.

2.0 DATA PRIVACY PRINCIPLES

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

2.1 TRANSPARENCY

The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data by Netsec, 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.

2.2 LEGITIMATE PURPOSE

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

2.3 PROPORTIONALITY

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

3.0 OPERATING GUIDELINE REQUIREMENTS

3.1 ACCOUNTABILITIES

3.1.1 Management

Following the three lines of defense model, the Management of Netsec is the First Line of Defense. Management owns the privacy risks intrinsic to its business and has the responsibility to manage these risks. Management is responsible for day-to-day compliance with this Guideline by maintaining effective internal controls (policies, procedures, and personnel) and risk management processes designed to manage privacy risks.

3.1.2 Data Protection Officer

The Data Protection Officer (DPO) is the Second Line of Defense. He is responsible for supporting the first line of defense in complying with the requirements of the DPA and related laws, and in testing the effectiveness pf first line's privacy processes and controls.

3.2 PROCESSES OF PERSONAL DATA/ PERSONAL DATA LIFE CYCLE

3.2.1 Collection

3.2.1.1 *Collection of Personal Information*

Netsec must not collect personal information, unless the information is reasonably necessary for, or directly related to, one or more of Netsec's functions or activities. Netsec may collect personal information only by lawful and fair means, and not in an unreasonably intrusive way.

Where it is reasonable and practical to do so, Netsec will collect personal information about an individual only from the individual alone. If, however, this information is collected from a third party, Netsec must act reasonably to ensure the individual is or has been made aware of the matters listed under 3.2.1.3 Components of Privacy Notice below.

3.2.1.2 *Collection of Sensitive Personal Information*

Netsec must only collect sensitive personal information: (i) Where the information is reasonably necessary for one or more of Netsec's functions or activities and with the individual's explicit consent; and (ii) if the collection is required by law.

Should collection of sensitive personal information of an individual be necessary, Netsec must take reasonable steps to ensure that the individual is aware of the matters listed under 3.2.1.3 Components of Privacy Notice below.

3.2.1.3. *Components of Privacy Notice*

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

a. Service Description

Netsec 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 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 Netsec

Netsec shall ensure that the identity and contact details of Netsec 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 DPO of Netsec 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

Netsec 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 appears to be obvious. Netsec 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

Netsec shall inform the data subject the collection methods of personal data attributes. Netsec shall provide clear explanations of all (obvious or nonobvious) personal data collection methods (direct or indirect).

e. Timing of Collection

Netsec 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

Netsec 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, Netsec shall clearly mark which purpose applies to which personal data attribute. Netsec shall provide the purpose for each personal data attribute in the notice. Netsec 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

Netsec should specify the data protection measures on storage, transmission, and reception of the personal data.

h. Method of Use

Netsec 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 Netsec intends to process the personal information in some way prior to using it for the stated purposes, Netsec shall provide relevant information to the data subject as to that processing.

i. Location of Personal Data

Netsec 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

Netsec shall give notice to data subjects on whether or not personal data will be transferred to a third party. If Netsec transfers personal data to a third party, it shall notify the data subject of recipient of such personal data. Although Netsec needs to identify and give notice of individual third-party recipients, Netsec may specify a group of recipients using clearly defined criteria where appropriate. If Netsec 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

Netsec 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. Netsec should specify the data protection measures on disposal of the personal data.

l. Participation and Rights of Data Subject

Netsec shall notify data subjects of their right to access their personal data possessed and/or controlled by Netsec, as well as their rights for the correction of personal data. Netsec 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), Netsec shall explain the reason for refusing to correct the information to the data subject.

Netsec shall indicate the following rights of data subject:

i. Right to access and correction. Netsec 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 Netsec will act on such complaint.
iii. Right to inquiry. Netsec shall provide the contact information for inquiries regarding the processing of personal information.

m. Intended Recipients of Personal Data

Netsec shall include the intended recipients or entities to which Netsec 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.

3.2.1.4 *Consent*

a. In circumstances where consent is needed, Netsec 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.

3.2.1.5 *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 3.2.1.1 Collection of personal information, 3.2.1.2 Collection of sensitive personal information, 3.2.1.3 Components of Privacy Notice and 3.2.1.4 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.

3.2.1.6 *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:

(i) The personal data is publicly available; or
(ii) 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.

3.2.1.7 *Collection of Personal Data for CCTV Surveillance*

a. Some of Netsec'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 Netsec's approved guidelines.

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

3.2.2 Usage

3.2.2.1 Personal data must be processed fairly and lawfully, 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.

3.2.2.2 As a general rule, Netsec's Management and employees must not use personal data about a 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 Netsec to use or disclose non-sensitive information for a secondary purpose, and the secondary purpose is related to the primary purpose; or
c. Netsec 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. Netsec reasonably believes that the use or disclosure is reasonably necessary for a specified purpose by or on behalf of an enforcement body; or

f. Netsec 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.

3.2.2.3 *Direct Marketing*

a. When contacting data subjects for direct marketing in whatever form, the following conditions must be present:

(i) Netsec provides simple means by which the data subject may easily request not to receive direct marketing communications from Netsec;

(ii) In each direct marketing communication with the data subject, Netsec 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;

(iii) The data subject has not made a request to Netsec not to receive direct marketing communications; and

(iv) Netsec 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:

(i) The information has been collected from the data subject and the data subject would reasonably expect Netsec to use it for that purpose; or

(ii) The information has been collected from a party other than the data subject and Netsec 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.

3.2.2.4 *Use of Government-Related Identifiers*

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

3.2.3 Access and Correction

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.

3.2.3.1 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.

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

a. Netsec 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 Netsec 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 Netsec on behalf of an enforcement body; or

j. Where the data subject:
- has been refused access to his/her personal data which Netsec 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.

3.2.4 Disclosure and Distribution/Data Sharing to Third Parties

3.2.4.1. 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 Netsec have:

a. Signed agreements to protect personal data consistent with this Guideline, 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 Netsec 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 Netsec.

3.2.4.2. *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
- Netsec 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 Netsec 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. Netsec 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).

3.2.5 Storage and Transmission

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

3.2.6 Retention

3.2.6.1 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.

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

3.2.6.3 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.

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

3.2.7 Disposal and Destruction

3.2.7.1 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.

3.2.7.2 Upon the expiration of identified lawful business purposes or withdrawal of consent, Netsec 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.

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

3.3 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.

3.3.1 Organizational Measures

Netsec considers the following measures for data protection:

3.3.1.1 *Compliance Monitoring and Reporting*

a. To ensure compliance with the DPA and the NPC, Netsec shall undertake the necessary steps as follows:

(i) Compliance with NPC registration requirements:
- Appointment and registration of a DPO, 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 Guideline, the DPA, its IRR and applicable laws and regulations. Refer to section 3.3.1.2 Data Privacy Office/Data Privacy Committee below.

(iii) Establishment of a this Guideline, which includes guidelines for the annual review and update thereof. Refer to section 3.3.1.6 Review of Privacy Operating Guideline 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 3.3.1.3 Conduct PIA below.

(vi) Conduct of training and awareness seminars to promote entity-wide compliance to applicable laws and regulations. Refer to section 3.3.1.4 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 Guideline 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.

3.3.1.2 *Data Privacy Committee*

Netsec recognizes the need to define governance for the data privacy initiatives. Responsibility and accountability shall be assigned to the Data Privacy Committee (DCC) for developing, documenting, implementing, enforcing, monitoring, and updating Netsec's Guideline.

DCC shall be composed of the following members:

(a) President, who shall act as Chairman
(b) Treasurer and Sales Director
(c) General Counsel and Administrative Director, who shall act as Secretary

(d) Technical Director
(e) Technical Manager - Services
(f) Project Management Head

3.3.1.3 *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.

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.

d. The PIA shall include:

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

(ii) Netsec 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 Netsec.

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

e. Netsec 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

Netsec's risk exposures. It must also ensure or check that candidates for PIA and those undergoing PIA were properly identified and tracked.

3.3.1.4 *Trainings/Seminars and Certifications*

a. Netsec 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 Netsec'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 Netsec
- Be delivered in an appropriate and effective manner
- Circulate essential information to relevant employees as soon as practical or if an urgent need arises

c. Netsec shall ensure the attendance and participation of employees in relevant trainings and orientations, as often as necessary.

d. Netsec shall support certifications on data privacy and security, whenever necessary.

3.3.1.5 *Duty of Confidentiality*

a. All employees and authorized representatives of contractors in the name of Netsec 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 Netsec 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 Netsec for an indefinite period and extends beyond any termination of their employment period or contract.

e. Netsec reserves the right to take disciplinary action, including termination of employment for violations of the Non-Disclosure Agreement.

3.3.1.6 *Review of Privacy Operating Guideline*

a. This Guideline 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 Guideline. In addition, the General Counsel shall review any conflict between this Guideline and any local law; and make recommendations to the Board of Directors who shall review and approve this Guideline at least on an annual basis.

3.3.2 Physical Security Measures

Netsec 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.

3.3.2.1 *Role of Data Privacy Committee*

a. The DPO, in coordination with the DCC, Administrative Department, and Distribution Centers, shall develop and implement policies and procedures for Netsec to monitor and limit access to, and activities in, the building property of Netsec, 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 the DCC, 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.

3.3.2.2 *Role of Employees and Contractors*

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

3.3.2.3 *Minimum Physical Security Policies and Procedures*

a. Format of personal data to be collected

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

b. Storage type and location

- All personal data stored by Netsec 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

- Netsec should strictly regulate access to personal data under its control. Approved access should be granted only to authorized personnel.
- Authorization should be governed by strict procedures contained in Netsec's policies and procedures, and formal contracts signed by the employees, contractors, and third parties.
- 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

- 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.
- Only persons issued with security clearances should have access to Netsec's rooms and facilities storing personal data, unless required by law or exception is duly approved by appropriate management.
- Netsec should maintain a log, from which it can be ascertained which room or facility is accessed, including when, where, and by whom. Netsec should regularly review the log records, including applicable procedures.
- 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.

e. Design of office space/ workstation

- 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

- 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, 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 Netsec, or to third parties

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

- disposal of files that contain personal data, whether such files are stored on paper, electronic media;
- 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
- disposal of personal data stored offsite.

3.3.3 Technical Security Measures

Netsec 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:

3.3.3.1 *Role of Data Protection Officer*

The DPO, in coordination with the DPC and Technical Department, shall continuously develop and evaluate Netsec's security policies and procedures from collection, usage, sharing, storage and disposal of Personal Data.

3.3.3.2 *Role of Employees and Contractors*

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

3.3.3.3 *Minimum Technical Security Policies and Procedures*

a. Access Controls

Netsec 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

Netsec shall use systems (e.g., intrusion detection system) to monitor security breaches and alert Netsec 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

Netsec 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

Netsec shall review security policies, conduct vulnerability assessments and perform penetration testing within Netsec on regular schedule to be prescribed by the appropriate department or business unit.

e. Backup, restoration and recovery of personal data

Netsec 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

Netsec 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:

- Patch management procedures
- Anti-virus and Malware protection
- Encryption
- Online access to personal data
- Emails
- Portable media
- Identity access management
- Software development and change management procedures
- Host security controls

3.4 SECURITY INCIDENT AND BREACH RESPONSE AND NOTIFICATION

3.4.1 Creation of a Data Breach Response Team

Selected Technical Engineers of Netsec, spearheaded by the Technical Director, shall comprise the Data Breach Response (DBR) Team and shall be responsible for ensuring immediate action in the event of security incident or personal data breach. The DBR 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.

The DBR Team shall clearly define responsibilities, to ensure timely action in the event of a security incident or personal data breach:

- 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.

3.4.2 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
- 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
- Periodical review of policies and procedures being implemented in Netsec

3.4.3 Procedure for Recovery and Restoration of Personal Data

Netsec 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.

3.4.4 Documentation and Reporting Procedure of Security Incidents or 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.

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.

a. Considerations in Notifying NPC

If it is a personal data breach, the extent of harm should be determined and the corresponding need to notify NPC and the impacted data subjects.

The DPO should assess the criteria below:

- Are the personal data subject of the breach any of the following? Sensitive personal information, or other information that may be used to enable identity fraud.
- Is there reason to believe that the information may have been acquired by an unauthorized person (whether internal or external)?
- Is the unauthorized acquisition likely to give rise to a real risk of serious harm to the data subject?

b. Assessment of Harm and Considerations in Notifying the Data Subjects

The potential damages caused by a data breach may include:

- Threat to personal safety
- Identity theft
- Financial loss
- Humiliation or loss of dignity, damage to reputation or relationship
- Loss of business and/or employment opportunities.

b. Containment

Immediately after the discovery of the breach, DBR Team shall take containment "quick-remedy" measures to prevent further data leak, loss, alteration, etc. In cases where the incident will not be reported to NPC, DBR Team will identify the needed actions, with the help of DPO and his delegate, which should be captured in the Privacy Incident Form. If reportable to NPC, the DPC will be involved.

Containment measures may include:

- Keeping the evidence of the date breach to facilitate investigation
- Stopping the system if the data breach is caused by a system failure
- Asking the impacted user to change his password
- Changing the system configuration to control access and use
- Considering the need for technical assistance to fix the system loopholes
- Ceasing or changing the access rights of individuals suspected to have committed or contributed to the breach
- Notifying the relevant law enforcement agencies, apart from NPC, if criminal activities are likely to be committed

c. Root Cause Analysis and Remediation

To be able to address the incident correctly, the root cause/s should be accurately and completely identified. In cases where the incident will not be reported to NPC, the DBR Team will identify the root cause, with the help of DPO. Such should be captured in the Privacy Incident Form. If reportable to NPC, the DPC will be involved.

Discuss the corrective and preventative actions to address the incident. Based on the root cause/s identified, the DPT shall determine the corrective and preventative actions,

a. Corrective actions rectify and improve the current situation. Examples: Correcting the inaccurate data
b. Requesting the unauthorized recipient to return or delete the wrongly sent confidential files
c. Preventative actions take into account the whole process/system or similar processes systems to prevent any recurrence. Examples: Sweeping the system for any similar issues; Reviewing the end-to-end process to identify and fix any other loopholes

d. Reporting

For data breaches assessed by the DPO as reportable to NPC, reporting should be done within seventy-two (72) hours from knowledge of the breach including the nature of the breach, sensitive personal information involved, the root causes and the actions taken. The affected data subjects are also notified within seventy-two (72) hours from knowledge of the breach, unless there is a reason to postpone or omit notification, subject to approval of the NPC. In general, same contents as notification of NPC but must include instructions on how data subject will get further assistance and information and recommendations to reduce the harm or negative consequences of the breach.

NPC may be notified by written or electronic means but Sun Life-PH must have confirmation that the notification has been received. Data subjects or affected individuals shall be notified

individually, by written or electronic means, unless allowed by the NPC to use alternative means. The DPO will work with the impacted business function to notify the NPC and impacted individuals of any data breaches.

3. Filings to the NPC

Apart from the data breaches reported to the NPC within 72 hours as explained in (d) above, the NPC requires the following filings:

(a) Registration of DPO and Data Processing Systems - DPO Registration is the process by which a Personal Information Controller (PIC) provides the NPC with relevant information regarding its data protection officer. After the Registration of the DPO, the PIC also registers its Data Processing Systems. Registration is required for all PICs/entities that meet the criteria under NPC Circular 17-01. The DPO and Compliance Staff submit the necessary registration documents to the NPC following the form provided by NPC Circular 17-01 and related advisories.

(b) Annual Incident Report - Annually, the DPO and Compliance Staff report to the NPC all security incidents along with personal data breaches. For security incidents not involving personal data. a report containing aggregated data shall constitute sufficient documentation. The DPO and Compliance Staff submit the report to the NPC for all registered entities, following the form provided by NPC Circular 16-03 and related advisories.

3.5 INQUIRIES AND COMPLAINTS

- The DPO of Netsec 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.
- Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of Netsec, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to Netsec at dataprotection@netsecph.com and briefly discuss the inquiry, together with their contact details for reference.
- Complaints shall be filed in three (3) copies, or sent to dataprotection@netsecph.com
- The DPO shall confirm with the inquiring party/complainant its receipt of the inquiry/complaint.