ANCHOR LAND

SECURITY INCIDENT MANAGEMENT POLICY

Section 1. Overview

This Policy is intended to guide the Company and all of its personnel in order to ensure compliance with data privacy law, its IRR, and other issuances of the NPC, and to ensure proper handling of personal data breaches and other security incidents involving personal data under the custody and control of the Company.

Section 2. Scope

This Policy shall cover all security incidents and personal data breaches involving any data processing systems of the Company and/or personal data under its custody or control.

Section 3. Definitions

The following terms shall have their corresponding meanings as provided below:

"*DPA*"	refers to Republic Act No. 10173, its IRR, and other relevant laws and issuances by the National Privacy Commission.
"*Personal data breach*"	refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of: 1. An *availability breach* resulting from loss, accidental or unlawful destruction of personal data; 2. *Integrity breach* resulting from alteration of personal data; and/or

	3. A *confidentiality breach* resulting from the unauthorized disclosure of or access to personal data.
"*Data Processing System*"	refers to a system or procedure by which personal data is collected and processed in an information and communications system, or a relevant filing system.
"*Data subject*"	refers to an individual whose personal data is processed.
"*Personal data*"	pertains to the collective term used to refer to personal information, sensitive personal information, and privileged information.
"*Personal information*"	refers to any information, on its own or when combined with other information, from which the identity of an individual is apparent or can be reasonably and directly ascertained.
"*Sensitive personal information*"	refers to 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 proceedings for any offense committed or alleged to have been committed by such individual, 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 is 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.
"*Privileged information*"	refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication.
"*Personal Information Controller*" or "PIC"	refers to a natural or juridical person that controls the processing or use of personal data. It includes a person

	who instructs another person to process personal data on its behalf.
"*Personal Information Processor*" or "PIP"	refers to a natural or juridical person to whom a personal information controller may outsource the processing of personal data under the latter's control or custody.
"*Privacy Impact Assessment*"	refers to a process meant to evaluate and manage the impact on privacy of a particular program, project, process, measure, system or technology product of a PIC or PIP.
"*Process owner*"	refers to the office that owns, administers, and/or manages a data processing system, or is the principal custodian of a particular personal data under the control or custody of the Company. It excludes offices or units of service providers.
"*Security incident*"	refers to an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place.

Section 4. Security Incident Response Team

There shall be a Security Incident Response Team (SIRT), which shall be responsible for investigating a suspected security incidents and personal data breaches.

The SIRT shall be headed by the Data Protection Officer who shall have the authority to make immediate decisions regarding critical action, if necessary. The team shall have four (4) other permanent members appointed by the Company's Chief Executive Officer (CEO). Other employees/personnel may be called on to join the team on a per incident basis when their expertise or background is appropriate and necessary to effectively address the incident, as recommended by the permanent members and approved by the CEO.

Section 5. Duties and Responsibilities

The team is generally responsible for the following:

1. Implementing security incident management policy of the PIC or PIP;
2. Managing security incidents and personal data breaches; and
3. Compliance by the PIC or PIP with the relevant provisions of the Act, its IRR, and all related issuances by the Commission on personal data breach management.

Further duties and responsibilities include:

1. Investigate, assess and evaluate security incidents and personal data breaches in coordination with all concerned departments of the Company;
2. Restore integrity to the Company's information and communication system;
3. Recommend mitigation and remedial measures to be performed by the Process Owner/s and other concerned departments;
4. Accomplish a written report detailing the actions taken in compliance with the DPA;
5. Serve as the contact person/s for all reports of security incidents or personal data breaches;
6. Act as custodian of all reports and documents submitted or prepared in relation to all security incidents and personal data breaches.

Section 6. Security Incident or Data Breach Notification

Any employee/s or person/s who become aware of or has reason to believe that a security incident or personal data breach has occurred must immediately notify the Security Incident Response Team via email at alhidataprivacy@anchorland.com.ph.

The security incident or data breach must involve personal data under the custody or control of the Company. It also includes those being processed by a service provider or any other authorized third party.

A person or a process owner who wishes to notify the SIRT of an incident shall submit an Incident Report, as prescribed by the SIRT. The notifying party must be able to provide the following information:

1. Name
2. Contact details (email address and contact number)
3. Details of the incident (if known)
    - 3.1.1. Date and time of incident
    - 3.1.2. Number of persons affected
    - 3.1.3. Name of department processing the information

Section 7. Investigation of Security Incidents or Data Breaches

The SIRT shall evaluate and assess all Incident Reports referred to them in the following manner:

1. The SIRT shall determine if additional members are necessary to investigate the reported security incident or data breach. If deemed necessary, the SIRT shall recommend the designation of additional members to the Company CEO.

2. The SIRT shall conduct its investigation of the incident based on the Incident Report. However, performance of additional or clarificatory action shall not be prohibited in order to obtain information critical to the investigation.

3. The investigation shall be completed within forty-eight (48) hours after all the information needed to carry out the investigation has been obtained. The SIRT must determine within this period whether or not a data breach has occurred, and if notification to the NPC is necessary.

4. Thereafter, the SIRT shall issue its Assessment Report which may be communicated to the Process Owner in relation to any initial or urgent recommendation by the SIRT. However, if the report contains recommendations or other matters that requires the attention of management, it shall be transmitted immediately to the latter for appropriate action.

Section 8. Mandatory Personal Data Breach Notification to the NPC and Data Subjects

Notification shall be required upon knowledge of or when there is a reasonable belief by the SIRT that a personal data breach requiring notification has occurred, under the following conditions:

1. It involves sensitive personal information or any *other information*[1] that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. There is reason to believe that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

Where there is uncertainty regarding the need to notify the NPC, the following additional factors shall be considered:

1. The likelihood of harm or negative consequences on the affected data subjects;
2. Notification could reduce the risks arising from the personal data breach reasonably believed to have occurred;
3. The data breach would li*k*ely affect national security, public safety, public order, or public health;
4. The data breach affects at least one hundred (100) individuals;
5. The personal data involved is required by applicable laws or rules to be confidential; and
6. The personal data belongs or refers to vulnerable groups.

The DPO shall notify the NPC within seventy-two (72) hours after the SIRT has determined that a confirmed data breach meets the conditions set out in this Section.

For this purpose, the DPO shall send a notification letter to the NPC via email. The DPO shall make sure to obtain a confirmation from the NPC that it has received the notification letter.

The Company must also notify the affected data subject within the same period, unless there are grounds recognized by law that allow the Company to forego with such notification.

In determining whether a valid ground exists for not notifying or postponing the notification of the affected data subjects, the Company, through the DPO, may consult with the NPC.

[1] "Other information" shall include, but not be limited to: data about financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN numbers; or other similar information, which may be made basis of decisions concerning the data subject, including the grant of rights or benefits.

The notification shall include, but not be limited to:

1. Nature of the breach;
2. Personal data possibly involved;
3. Measures taken to address the breach;
4. Measures taken to reduce the harm or negative consequences of the breach;
5. Representative of the PIC, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
6. Any assistance to be provided to the affected data subjects.

Section 9. Reportorial Requirements

All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements.

Forms for this purpose shall be developed to guide the responsible parties in its accomplishment.

Any or all reports shall be made available when requested by the NPC. Provided, that a summary of all reports shall be submitted to the NPC annually, comprised of general information including the number of incidents or breach encountered, classified according to their impact on the availability, integrity, or confidentiality of personal data.

Section 10. Confidentiality

All information gathered or generated in the investigation and handling of security incidents or personal data breaches shall be held strictly in confidence, and shall not be disclosed, reproduced or disseminated to any third person, unless otherwise provided under this Policy and to the extent allowed under the DPA.

All information shall be made available only to those officers, employees, representatives and professional advisers of the Company who have a need-to-know of such information for the purpose stated in this Policy.

Section 11. Preventive or Minimization Measures

To prevent or minimize the occurrence of personal data breach, the following safeguards shall be adopted by the Company:

1. Conduct a privacy impact assessment (PIA) on the data processing systems involved in a security incident to identify attendant risks in the processing of personal data.
2. Regular review of the policies and procedures for security incident management, including the testing, assessment, and evaluation of the effectiveness of the security measures.
3. Implement appropriate security measures, change, and/or upgrade the existing ones to protect the availability, integrity and confidentiality of personal data being processed.
4. Conduct regular monitoring for security breaches.
5. Conduct capacity building of personnel to ensure knowledge of data breach management principles, and internal procedures for responding to security incidents.

Section 11. Penalties

Failure to comply with this Policy may subject the erring party to disciplinary action, in accordance with the applicable Code of Discipline, and other relevant rules and regulations. The Company reserves the right to exercise any other legal remedies available to it under all applicable laws, policies, rules and regulations.

Section 12. Review

This Policy shall be amended and updated every two (2) years, unless special circumstances requires a shorter period, or to comply with new and existing relevant DPA laws, rules, regulations and issuances by the NPC.

Section 13. Effectivity

Upon approval by the Board, this Policy and any subsequent amendment thereto shall take effect immediately after it has been posted in the Company's official website.

Prepared By:	Reviewed by:	Approved by:
Marydale C. Manato Data Protection Officer	**Sarah Joelle C. Lintag** Head, Corporate Affairs Department	**Mr. Steve Li** CEO