ANCHOR LAND

PRIVACY IMPACT ASSESSMENT

(Department)

Name of Organization:	Anchor Land Holdings, Inc.	
Department:		
Data Processing System/Program/Project:		
Process Owner/Department Head:		
Data Protection Officer::	Marydale C. Manato	alhidataprivacy@anchorland.com.ph

Table of Contents

OVERVIEW

A Privacy Impact Assessment (PIA) is an instrument for assessing the potential impacts on privacy of a process, information system, program, software module, device or other initiative which processes personal information and in consultation with stakeholders, for taking actions as necessary to treat privacy risk.[1]

Anchor Land Holdings, Inc. (ALHI) recognizes its responsibility to observe proactive approach to the management of risks represented by personal data processing by ensuring that the rights of data subjects are protected. To demonstrate its compliance with the Data Privacy Act, its Implementing Rules and Regulations, and related issuances of the NPC, ALHI undertakes to conduct a privacy impact assessment in its organization with the participation of the different process owners and stakeholders.

I. Project/System Description

a. Description

Describe the program, project, process, measure, system or technology product and its

[1] NPC Privacy Toolkit. Privacy Impact Assessment.

context. Define and specify what it intends to achieve. Consider the pointers below to help you describe the project.

Brief Description of the project/system	The system/project's overall aims (purpose of the project/system)	Any related documents to support the projects/system
Guide questions: *Describe the process of the projects* *Describe the scope and extent* *Any links with existing programs or other projects*	*Guide questions:* *What is the project/system aims to achieve?* *What are the benefits for the organizations and data subjects?*	*Guide questions:* *Project/System Requirements Specification* *Project/System Design Specification* *Or any related documents*

b. Scope of the PIA

This section should explain what part or phase of the program the PIA covers and, where necessary for clarity, what it does not cover.

What will the PIA cover?	
What areas are outside scope?	
Is this just a "desk-top" information gathering exercise, do I have to get information from a wide variety of sources?	
Who needs to be involved and when will they be available?	

Where does the PIA need to fit in the overall project plan and timelines?	
Who will make decisions about the issues identified by the PIA? What information do they need and how long will it take to get sign-off from them?	
Do I need to consult with anyone (for instance the individuals whose personal information the project will involve)? When and how should this happen?	
Are there any third parties involved and how long do I need to allow for them to play their part?	

II. Threshold Analysis

The following questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

	Question	Yes/No	Comments
1.	Will the project involve the collection of new information about individuals?		
2.	Is the information about individuals sensitive in nature and likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?		
3.	Are you using information about individuals for a purpose it is not currently		

	used for, or in a way it is not currently used?		
4.	Will the initiative require you to contact individuals in ways which they may find intrusive?		
5.	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		
6.	Does the initiative involve you using new technology which might be perceived as being privacy intrusive (e.g. biometrics or facial recognition)?		
7.	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		
8.	Are the personal data collected prior to August 2016?		
9.	From your answers above, is your conclusion that a PIA is required? (If no, please explain why in the comments column)		

III. Stakeholder(s) Engagement

State all project stakeholders, consulted in conducting PIA. Identify which part they were involved. (Describe how stakeholders were engaged in the PIA process)

**add additional rows if needed*

Name	Role	Involvement	Inputs/ Recommendations
*			

IV. Personal Data Flows

This is to identify what personal information will be used in the project or initiative and how it will be collected, used and managed. It will help in identifying any areas of risk.

Type of Personal Information Description of information that relates to individuals (*e.g. Personal Full Name, address, gender, phone number, etc.*)	**If Sensitive Personal Information, state which type** Sensitive personal information consists of data on (*e.g. race, ethnic origin, health, marital status, criminal offences or allegations, religious beliefs, political beliefs, sex life, government issued numbers*)	**Source of the data** Where does the information come from? (*e.g. from applicants, from employees, from customers, etc.*)	**Purpose, Use and Storage, Retention** What is the data used for? Where/How is it stored? How long is the data retained?	**Disclosure and Access** Who is the data disclosed to, or who has access to it? (both internal and external)	**Disposal/Destruction** How will the data be disposed? Who will facilitate the destruction of the data?

*					

**add additional rows if needed*

V. Privacy Impact Analysis

Each program, project or means for collecting personal information should be tested for consistency with the following Data Privacy Principles (as identified in Rule IV, Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012").

Respond accordingly with the questions by checking either the "Yes" or "No" column ***and/or listing what the questions may indicate****.*

Transparency	Yes	No	Not applicable
1. Are data subjects aware of the nature, purpose, and extent of the processing of his or her personal data?			
2. Are data subjects aware of the risks and safeguards involved in the processing of his or her personal data?			
3. Are data subjects aware of his or her rights as a data subject and how these can be exercised? Below are the rights of the data subjects: • Right to be informed • Right to object • Right to access • Right to correct • Right for erasure or blocking • Right to file a complaint • Right to damages • Right to data portability			
4. Is there a document available for public review that sets out the policies for the management of personal data? *Please identify document(s) and provide link where available:*			

5. Are there steps in place to allow an individual to know what personal data it holds about them and its purpose of collection, usage and disclosure?			
6. Are the data subjects aware of the identity of the personal information controller or the organization/entity processing their personal data?			
7. Are the data subjects provided information about how to contact the organization's Data Protection Officer (DPO)?			

Legitimate Purpose	Yes	No	Not applicable
1. Is the processing of personal data compatible with a declared and specified purpose which are not contrary to law, morals, or public policy?			
2. Is the processing of personal data authorized by a specific law or regulation, or by the individual through express consent?			
Proportionality	**Yes**	**No**	**Not applicable**
1. Is the processing of personal data adequate, relevant, suitable, necessary and not excessive in relation to a declared and specified purpose?			
2. Is the processing of personal data necessary to fulfill the purpose of the processing and no other means are available?			
Collection	**Yes**	**No**	**Not applicable**
1. Is the collection of personal data for a declared, specified and legitimate purpose?			
2. Is individual consent secured prior to the collection and processing of personal data? If no, specify the reason			
3. Is consent time-bound in relation to the declared, specified and legitimate purpose?			

4. Can consent be withdrawn?			
5. Are all the personal data collected necessary for the program?			
6. Are the personal data anonymized or de-identified?			
7. Is the collection of personal data directly from the individual?			
8. Is there authority for collecting personal data about the individual from other sources?			
9. Is it necessary to assign or collect a unique identifier to individuals to enable your organization to carry out the program?			
10. Is it necessary to collect a unique identifier of another agency? e.g. SSS number, PhilHealth, TIN, Pag-IBIG, etc.,			
Use and Disclosure	Yes	No	Not applicable
1. Will Personal data only be used or disclosed for the primary purpose?			
2. Are the uses and disclosures of personal data for a secondary purpose authorized by law or the individual?			
Data Quality	Yes	No	Not applicable
1. Please identify all steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date:			
1.1 *Please identify all steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date:			
1.2 *The system is regularly tested for accuracy			
1.3 *Periodic reviews of the information			

1.4 *A disposal schedule in place that deletes information that is over the retention period			
1.5 *Staff are trained in the use of the tools and receive periodic updates			
1.6 *Reviews of audit trails are undertaken regularly			
1.7 *Independent oversight			
1.8 *Incidents are reviewed for lessons learnt and systems/ processes updated appropriately			
1.9 *Others, please specify			
Data Security	Yes	No	Not applicable
1. Do you have appropriate and reasonable organizational, physical and technical security measures in place? *Organizational measures - refer to the system's environment, particularly to the individuals carrying them out. Implementing the organizational data protection policies aim to maintain the availability, integrity, and confidentiality of personal data against any accidental or unlawful processing (i.e. access control policy, employee training, surveillance, etc.,)* *Physical measures – refers to policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media (i.e. locks, backup protection, workstation protection, etc.,)* *Technical measures - involves the technological aspect of security in protecting personal information (i.e. encryption, data center policies, data transfer policies, etc.,)*			
Organizational Security	Yes	No	Not applicable
*Have you appointed a data protection officer or compliance officer?			

*Are there any data protection and security measure policies in place?			
*Do you have an inventory of processing systems? Will you include this project/system?			
*Are the users/staffs that will process personal data through this project/system under strict confidentiality if the personal data are not intended for public disclosure?			
*If the processing is delegated to a Personal Information Processor, have you reviewed the contract with the personal information processor?			
Physical Security	Yes	No	Not applicable
*Are there policies and procedures to monitor and limit the access to this project/system?			
*Are the duties, responsibilities and schedule of the individuals that will handle the personal data processing clearly defined?			
*Do you have an inventory of processing systems? Will you include this project/system?			
Technical Security	Yes	No	Not applicable
*Is there a security policy with respect to the processing of personal data?			
*Do you have policies and procedures to restore the availability and access to personal data when an incident happens?			
*Do/Will you regularly test, assess and evaluate the effectiveness of the security measures of this project/ system?			
*Are the personal data processed by this project/system encrypted while in transit or at rest?			
2. The program has taken reasonable steps to protect the personal data it holds from misuse and loss and from unauthorized access, modification or disclosure?			
3. If yes, which of the following has the program undertaken to protect personal data across the information lifecycle:			

3.1 * Identifying and understanding information types			
3.2 * Assessing and determining the value of the information			
3.3 * Identifying the security risks to the information			
3.4 * Applying security measures to protect the information			
3.5 * Managing the information risks.			
Disposal	Yes	No	Not applicable
1. The program will take reasonable steps to destroy or de- identify personal data if it is no longer needed for any purpose. If YES, please list the steps ____			
Cross-border Data Flows (optional)	Yes	No	Not applicable
1.The program will transfer personal data to an organization or person outside of the Philippines If YES, please describe			
2.Personal data will only be transferred to someone outside of the Philippines if any of the following apply: a. The individual consents to the transfer; b. The organization reasonably believes that the recipient is subject to laws or a contract enforcing information handling principles substantially similar to the DPA of 2012; c. The transfer is necessary for the performance of a contract between the individual and the organization; d. The transfer is necessary as part of a contract in the interest of the individual between the organization and a third party; or e. The transfer is for the benefit of the individual.			

3. The organization has taken reasonable steps so that the information transferred will be stored, used, disclosed and otherwise processed consistently with the DPA of 2012. If YES, please describe			

VI. Privacy Risk Management

For the purpose of this section, a **risk** refers to the potential of an incident to result in harm or danger to a data subject or organization. Risks are those that could lead to the unauthorized collection, use, disclosure or access to personal data. It includes risks that the confidentiality, integrity and availability of personal data will not be maintained, or the risk that processing will violate rights of data subjects or privacy principles (transparency, legitimacy and proportionality).

The first step in managing risks is to identify them, including threats and vulnerabilities, and by evaluating its impact and probability.

The following definitions are used in this section,

Risk - "the potential for loss, damage or destruction as a result of a threat exploiting a vulnerability";

Threat - "a potential cause of an unwanted incident, which may result in harm to a system or organization";

Vulnerability - "a weakness of an asset or group of assets that can be exploited by one or more threats";

Impact - severity of the injuries that might arise if the event does occur (can be ranked from trivial injuries to major injuries); and

Probability - chance or probability of something happening;

Impact		
Rating	Types	Description

1	Negligible	The data subjects will either not be affected or may encounter a few inconveniences, which they will overcome without any problem.
2	Limited	The data subject may encounter significant inconveniences, which they will be able to overcome despite a few difficulties.
3	Significant	The data subjects may encounter significant inconveniences, which they should be able to overcome but with serious difficulties.
4	Maximum	The data subjects may encounter significant inconveniences, or even irreversible, consequences, which they may not overcome.

Probability		
1	Unlikely	Not expected, but there is a slight possibility it may occur at some time.
2	Possible	Casual occurrence. It might happen at some time.
3	Likely	Frequent occurrence. There is a strong possibility that it might occur.
4	Almost Certain	Very likely. It is expected to occur in most circumstances.

Select the appropriate level or criteria of impact and probability to better assess the risk. Kindly refer to the table below for the criteria.

Note: Try to itemize your risks by designating a reference number. This will be used as a basis on the next sections (VII. Recommended Privacy Solutions and VIII. Sign off and Action Plan). Also, ***base the risks on the violation of privacy principles, rights of data subjects and confidentiality, integrity and availability of personal data****.*

Ref#	Threats/ Vulnerabilities	Impact				Probability				Risk Rating	
	**Organizational security measures not instituted	1	2	3	4	1	2	3	4		
	**Physical security measures not implemented	1	2	3	4	1	2	3	4		
	**Technical security measures not	1	2	3	4	1	2	3	4		

	installed										
	***Privacy rights not respected*	1	2	3	4	1	2	3	4		
	***Privacy principles undermined*	1	2	3	4	1	2	3	4		
	***Lawful criteria to process PI not applied*	1	2	3	4	1	2	3	4		
	***Conditions to process SPI not applied*	1	2	3	4	1	2	3	4		
	***Data Sharing condition not applied*	1	2	3	4	1	2	3	4		

**add additional rows if needed*

***texts in red font are just examples; you may change/add/amend/delete as necessary and applicable.*

Kindly follow the formula below for getting the Risk Rating:

Risk Rating = Impact x Probability

Kindly refer to the table below for the criteria.

Rating	Types
1	Negligible
2 to 4	Low Risk
6 to 9	Medium Risk
10-16	High Risk

Privacy Risk Map

Level of Impact	Identified Risks (Violation)			
4-Maximum	****Negligence in access of PI, SPI***		****Unauthorized disclosure***	****Intentional breach***

3-Significant	**Improper disposal of data store*			
2-Limited		**Unauthorized change of PI, SPI*		
1-Negligible	**Unauthorized purpose*			
	1-Unlikely	2-Possible	3-Likely	4-Almost certain
	Likelihood (Probability)			

**texts in red font are just examples; you may change/add/amend/delete as necessary and applicable.*

VII. Recommended Privacy Solutions

From the risks stated in the previous section, identify the recommended solution or mitigation measures. You can cite your existing controls to treat the risks in the same column.

Risk	**Recommended Solutions** (Please provide justification)	**Result:** is the risk eliminated, reduced, or accepted?

**add additional rows if needed*

VIII. Sign Off and Action Plan

Please use the checklist below to confirm that all stages in the PIA have been completed and to record any actions agreed.

PIA Stage	Actions Required	Complete? (Y/N)	Brief summary of any issues identified
I. Project/System Description	Complete Template.		

II. Threshold Analysis	Complete screening questions and decide to undertake PIA.		
III. Stakeholder(s) Engagement	Complete Template to determine the participation of stakeholders in the PIA process.		
IV. Personal Data Flows	Complete Template. Use outcome to begin to consider privacy issues.		
V. Privacy Impact Analysis	Complete Template. Use outcome to test compliance with the Data Privacy Principles.		
VI. Privacy Risk Management	Complete Template. Use outcome to identify risks.		
VII. Recommended Privacy Solutions	Complete Template. Agree mitigating actions.		

Risk	Approved Solution	Solution Approved by

**add additional rows if needed.*

Prepared by: Process Owner/Department Head	
Name:	
Job Title:	
Signature:	
Date:	

Noted by: Data Protection Officer	
Name:	
Job Title:	
Signature:	
Date:	

Approved by: Chief Executive Officer (CEO)	
Name:	Mr. Steve Li
Job Title:	CEO
Signature:	
Date:	