HARBOR STAR
SHIPPING SERVICES, INC.

Subject:	**Data Privacy Policy**	Policy No.:	HRDM-2018-001
Prepared by:	Effel T. Santillan	Revision No.:	-
Revised by:	-	Date Revised:	-
Endorsed by:	Data Privacy Committee	Date Approved:	14 August 2018
Approved by:	Geronimo P. Bella, Jr.	Effectivity Date:	01 September 2018

1.0 Objective

1.1 To ensure compliance to the Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) and its Implementing Rules and Regulations (IRR).

1.2 To ensure proper procedures are in place for the processing and management of personal data assuring individuals that their personal data is processed in accordance with the data privacy principles, that their data is secure at all times and safe from unauthorized access, alteration, use or loss.

1.3 To know that there is someone within the Company who has specific responsibility and knowledge about data protection compliance.

1.4 To inform all employees of their responsibilities when processing personal data, and that methods of handling that information is clearly understood.

1.5 To ensure that other organizations with whom the Company data needs to be shared or transferred, meet compliance requirements.

1.6 To ensure any new systems being implemented are assessed on whether they will hold personal data, whether the system presents any risks, damage or impact to individuals' data and that it meets this policy.

2.0 Coverage

2.1 This policy applies to all personal data and sensitive personal data collected and processed by the Company in the conduct of its business, in electronic format in any medium and within structured paper filing systems.

2.2 This policy applies to all employees of the Company, its subsidiaries and clients.

3.0 Terms and Definition

Term	**Definition**
Company	Harbor Star Shipping Services Inc.
Data Breach	Is a security incident that (a) leads to unlawful or unauthorized processing of personal data; (b) compromises the availability, integrity or confidentiality of personal data
Data Privacy Act or DPA	refers to Republic Act No. 10173 or the Data Privacy Act of 2012 and its implementing rules and regulations
Data Protection Officer ("DPO")	Appointed by the Company. The DPO is responsible for ensuring the Company's compliance with applicable laws and regulations for the protection of data privacy and security.
Data sharing	Disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal

	information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor.
Data Subject	refers to an individual whose Personal Information, Sensitive Personal Information, or Privileged Information is processed
Employees	All persons in the employ of the company regardless of status
HRDM	Human Resources Development and Management
Immediate Head	Immediate superior of requesting employee who is a Department/Division Head or President as the case may be
National Privacy Commission (NPC)	The National Privacy Commission is the country's privacy watchdog; an independent body mandated to administer and implement the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection.
Personal Information	refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual
Personal information processor	refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject
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 may be performed through automated means, or manual processing, if the Personal Data are contained or are intended to be contained in a filing system
Sensitive Personal Information	Refers to Personal Data: 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, or to any proceeding 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.

4.0 Responsibilities

4.1 The following shall be held responsible and accountable to ensure the policies are implemented and complied with by all concerned:

4.1.1 Data Protection Officer

4.1.2 HRDM Head

4.1.3 Department/Division Heads

4.2 Any irregularity or violation shall be reported to HRDM.

5.0 Guidelines

5.1 A Data Protection Officer ("DPO") shall The DPO's functions and responsibilities shall particularly include, among others:

5.1.1 Monitor compliance;

5.1.2 Ensure conduct of Privacy Impact Assessment (PIA);

5.1.3 Ensure data subjects rights are respected;

5.1.4 Ensure Proper breach management;

5.1.5 Cultivate internal awareness on data privacy;

5.1.6 Advocate a privacy by design approach;

5.1.7 Serve as contact person for privacy matters;

5.1.8 Serve as conduit with the National Privacy Commission;

5.1.9 Perform other duties as may be defined.

5.2 **Data Privacy Principles -** All Processing of Personal Data within the Company should be conducted in compliance with the following data privacy principles as indicated in the Data Privacy Act:

5.2.1 ***Transparency.*** The data subject must be aware of the nature, purpose, and extent of the processing of individual's personal data, including the risks and safeguards involved, the identity of personal information controller, 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.

5.2.2 ***Legitimate purpose.*** The Processing of Personal Data by the Company shall be compatible with a declared and specified purpose that must not be contrary to law, morals, or public policy.

5.2.3 ***Proportionality.*** The Processing of Personal Data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. The Company shall process personal Data only if the purpose of the processing could not be reasonably fulfilled by other means.

5.3 **Data Processing Records -** Adequate records of the Company's Personal Data Processing activities shall be maintained at all times. The DPO, with the cooperation and assistance of all the concerned departments involved in the Processing of Personal Data, shall be responsible for ensuring that these records are kept up-to-date. These records shall include, at the minimum:

5.3.1 Information about the purpose of the Processing of Personal Data, including any intended future Processing or data sharing;

5.3.2 A description of all categories of Data Subjects, Personal Data, and recipients of such Personal Data that will be involved in the Processing;

5.3.3 General information about the data flow within the Company, from the time of collection and retention, including the time limits for disposal or erasure of Personal Data;

5.3.4 A general description of the organizational, physical, and technical security measures in place within the Company; and

5.3.5 The name and contact details of the DPO, Personal Data processors, as well as any other staff members accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

5.4 **Management of Human Resources** - The DPO, with the cooperation of HRDM department, shall develop and implement measures to ensure that all the Company's staff who have access to Personal Data will strictly process such data in compliance with the requirements of the Data Privacy Act and other applicable laws and regulations. These measures may include drafting new or updated relevant policies of the Company and conducting training programs to educate employees on data privacy related concerns.

5.5 **Data Collection** - The DPO, with the assistance of HRDM Head, shall ensure that Company shall obtain the employee's informed consent, evidenced by a signed Personal Data Processing and Sharing Consent form *(Attachment 1)*. This shall also be regularly monitored, modified, and updated to ensure that the rights of the Data Subjects are respected, and that Processing thereof is done fully in accordance with the DPA and other applicable laws and regulations.

5.6 **Data Retention -** Subject to applicable requirements of the DPA and other relevant laws and regulations, Personal Data shall not be retained by the Company for a period longer than necessary and/or proportionate to the purposes for which such data was collected. The DPO, with HRDM Head and any other departments of the Company responsible for the Processing of Personal Data, shall be responsible for developing measures to determine the applicable data retention schedules, and procedures to allow for the

withdrawal of previously given consent of the Data Subject, as well as to safeguard the destruction and disposal of such Personal Data in accordance with the DPA and other applicable laws and regulations.

5.7 The DPO, with the assistance of HRDM Head and Support Services Division Head, shall develop and implement policies and procedures for the Company to monitor and limit access to, and activities in, the offices of HRDM, as well as any other departments and/or workstations in the Company where Personal Data is processed, including guidelines that specify the proper use of, and access to, electronic media.

5.8 The design and layout of the office spaces and work stations of the abovementioned departments, including the physical arrangement of furniture and equipment, shall be periodically evaluated and readjusted in order to provide privacy to anyone Processing Personal Data, taking into consideration the environment and accessibility to unauthorized persons.

5.9 The duties, responsibilities, and schedules of individuals involved in the Processing of Personal Data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time. Further, the rooms and workstations used in the Processing of Personal Data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

5.10 The DPO, with the cooperation and assistance of ICT, shall continuously develop and evaluate the Company's security policy with respect to the Processing of Personal Data. The security policy should include the following minimum requirements:

5.10.1 Safeguards to protect the Company's computer network and systems against accidental, unlawful, or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access;

5.10.2 The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of the Company's data processing systems and services;

5.10.3 Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in the Company's computer network and system, and for taking preventive, corrective, and mitigating actions against security incidents that can lead to a Personal Data breach;

5.10.4 The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

5.10.5 A process for regularly testing, assessing, and evaluating the effectiveness of security measures; and

5.10.6 Encryption of Personal Data during storage and while in transit, authentication process, and other technical security measures that control and limit access thereto.

5.11 As provided under the DPA, Data Subjects have the following rights in connection with the Processing of their Personal Data: right to be informed, right to object, right to access, right to rectification, right to erasure or blocking, and right to damages. Employees and agents of the Company are required to strictly respect and obey the rights of the Data Subjects. The DPO, with the assistance of HRDM shall be responsible for monitoring such compliance and developing the appropriate disciplinary measures and mechanism.

5.12 The Data Subject has the right to be informed whether Personal Data pertaining to the employee shall be, are being, or have been processed.

5.13 The Data Subject shall be notified and furnished with information indicated hereunder before the entry of his or her Personal Data into the records of the Company, or at the next practical opportunity:

5.13.1 Description of the Personal Data to be entered into the system;

5.13.2 Purposes for which they are being or will be processed, including Processing for direct marketing, profiling or historical, statistical or scientific purpose;

5.13.3 Basis of Processing, when Processing is not based on the consent of the Data Subject;

5.13.4 Scope and method of the Personal Data Processing;

5.13.5 The recipients or classes of recipients to whom the Personal Data are or may be disclosed or shared;

5.13.6 Methods utilized for automated access, if the same is allowed by the Data Subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;

5.13.7 The identity and contact details of the DPO;

5.13.8 The period for which the Personal Data will be stored; and

5.13.9 The existence of their rights as Data Subjects, including the right to access, correction, and to object to the Processing, as well as the right to lodge a complaint before the National Privacy Commission.

5.14 The Data Subject shall have the right to object to the Processing of his or her Personal Data, including Processing for direct marketing, automated Processing or profiling. The Data Subject shall also be notified and given an opportunity to withhold consent to the Processing in case of changes or any amendment to the information supplied or declared to the Data Subject in the preceding paragraph.

5.15 When a Data Subject objects or withholds consent, the Company shall no longer process the Personal Data, unless:

5.15.1 The Personal Data is needed pursuant to a subpoena;

5.15.2 The Processing is for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the Data Subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the Company and the Data Subject; or

5.15.3 The Personal Data is being collected and processed to comply with a legal obligation.

5.16 The Data Subject has the right to reasonable access to, upon demand, the following:

5.16.1 Contents of his or her Personal Data that were processed;

5.16.2 Sources from which Personal Data were obtained;

5.16.3 Names and addresses of recipients of the Personal Data;

5.16.4 Manner by which his or her Personal Data were processed; Reasons for the disclosure of the Personal Data to recipients, if any;

5.16.5 Information on automated processes where the Personal Data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the Data Subject;

5.16.6 Date when Personal Data concerning the Data Subject were last accessed and modified; and

5.16.7 The designation, name or identity, and address of the DPO.

5.17 The Data Subject has the right to dispute the inaccuracy or rectify the error in his or her Personal Data, and the Company shall correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the Personal Data has been corrected, the Company shall ensure the accessibility of both the new and the retracted Personal Data and the simultaneous receipt of the new and the retracted Personal Data by the intended recipients thereof: Provided, That recipients or third parties who have previously received such processed Personal Data shall be informed of its inaccuracy and its rectification, upon reasonable request of the Data Subject.

5.18 The Data Subject shall have the right to suspend, withdraw, or order the blocking, removal, or destruction of his or her Personal Data from the Company's filing system. This right may be exercised upon discovery and substantial proof of any of the following:

5.18.1 The Personal Data is incomplete, outdated, false, or unlawfully obtained;

5.18.2 The Personal Data is being used for purpose not authorized by the Data Subject;

5.18.3 The Personal Data is no longer necessary for the purposes for which they were collected;

5.18.4 The Data Subject withdraws consent or objects to the Processing, and there is no other legal ground or overriding legitimate interest for the Processing by the Company;

5.18.5 The Personal Data concerns private information that is prejudicial to Data Subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;

5.18.6 The Processing is unlawful; or

5.18.7 The Data Subject's rights have been violated.

5.19 The DPO may notify third parties who have previously received such processed Personal Data that the Data Subject has withdrawn his or her consent to the Processing thereof upon reasonable request by the Data Subject.

5.20 The lawful heirs and assigns of the Data Subject may invoke the rights of the Data Subject to which he or she is an heir or an assignee, at any time after the death of the Data Subject, or when the Data Subject is incapacitated or incapable of exercising his/her rights.

5.21 Whenever Personal Data is processed by the Company through electronic means and in a structured and commonly used format, the Data Subject shall have the right to obtain a copy of such data in an electronic or structured format that is commonly used and allows for further use by the Data Subject. The exercise of this right shall primarily take into account the right of Data Subject to have control over his or her Personal Data being processed based on consent or contract, for commercial purpose, or through automated means. The DPO shall regularly monitor and implement the National Privacy Commission's issuances specifying the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

5.22 **Data Breaches and Security Incident** - All employees and crew are tasked with regularly monitoring for signs of possible data breach or Security Incident. In the event, that such signs are discovered, they shall immediately report the facts and circumstances to the DPO within 72 hours upon knowledge of, or when there is reasonable belief that a personal data breach has occurred. The obligation remains with the personal information controller even if the processing information is outsourced or subcontracted.

5.23 **Breach Reports** - All relevant Security incident and Personal Data breaches shall be documented in the NCPAR (Non-Conformity, Corrective and Preventive Action Report System) where involved employees may be subjected to further disciplinary action. These reports shall be made available when requested by the National Privacy Commission. A general summary of the reports shall be submitted by the DPO to the National Privacy Commission annually.

5.24 When engaging to third party agent/entity (e.g. outsourcing and subcontracting agreements, suppliers, clients) and there is personal data processing involved, this should be documented thru the Data Sharing Agreement *(Attachment 2)*, this is a stand-alone document aside from any contractual agreement made by the Company and the respective third party.

6.0 Penalties

6.1 Violation of any provision in this policy not specifically penalized herein or by the Company's Code of Discipline can be imposed a penalty of verbal or written warning, reprimand, suspension or termination of employment, as the circumstances may warrant. Further, the Company reserves the right to avail of remedies allowed by law to protect its employees, properties and other interests.

7.0 Forms and Annexes

7.1 Attachment 1: Personal Data Processing and Sharing Consent Form

7.2 Attachment 2: Data Sharing Agreement

8.0 Repealing Clause

8.1 The President reserves the right to alter, revise, amend, revoke, or waive any provision in this policy with the end view of doing what is right and just under the circumstances.

8.2 All directives, practices and orders contrary to this order are hereby superseded and revoked.

Approved by:

Geronimo P. Bella, Jr.
President