BRIGHT MARITIME CORPORATION

COMPANY POLICY ON DATA PRIVACY

In connection with the enactment of Republic Act No. 10173 or the Data Privacy Act of 2012 and its implementing rules and regulations, Bright Maritime Corporation **("BMC")** introduces and implements this Policy, adopting relevant provisions of said Act and its implementing rules and regulations.

This Policy shall take effect on 12 December 2018.

I. DEFINITION OF TERMS

a. *Data Privacy Act or DPA* - refers to Republic Act No. 10173 or the Data Privacy Act of 2012 and its implementing rules and regulations.

b. *Commission* - refers to the National Privacy Commission, the government agency principally in charge of implementation and enforcement of the DPA.

c. *Data Subject* - is defined as the individual whose personal data is processed.

d. *Personal Data* – refers to Personal Information, Sensitive Personal Information, and Privileged Information belonging to Data Subject.

e. *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.

f. *Privileged Information* - any and all forms of Personal Data, which, under the Rules of Court and other pertinent laws constitute privileged communication.

g. *Sensitive Personal* - Information refers to Personal Data regarding:

   1. Data Subject's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

   2. Data Subject'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. Information 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. Information specifically established by an executive order or an act of Congress to be kept classified.

h. *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.

i. *Personal information controller ("PIC")* – an employee who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

1. A person or organization who performs such functions as instructed by another person or organization; and

2. An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

PIC, for purposes of this Policy, may also refer to BMC or its employer performing the functions and responsibilities of a PIC.

j. *Personal information processor ("PIP")* - any natural or juridical person qualified to act as such under the DPA to whom BMC may outsource the processing of Personal Data pertaining to a Data Subject.

k. *Consent of the Data Subject* - freely given, specific, informed indication of will, whereby the Data Subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the Data Subject by an agent specifically authorized by the Data Subject to do so.

l. *Filing system* - any information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, it is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.

m. *Information and Communications System* - a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded,

transmitted or stored and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document.

n. *Security Incident* - an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of Personal Data, including those that would result in a Personal Data breach, if not for the safeguards put in place.

II. SCOPE

This Policy covers all types of processing involving Personal Data, except the following:

a. Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

   1. The fact that the individual is or was an officer or employee of the government institution;

   2. The title, business address and office telephone number of the individual;

   3. The classification, salary range and responsibilities of the position held by the individual; and

   4. The name of the individual on a document prepared by the individual in the course of employment with the government;

b. Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

c. Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;

d. Personal information processed for journalistic, artistic, literary or research purposes;

e. Information necessary in order to carry out the functions of public authority which includes the processing of Personal Data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions.

f. Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and

g. Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

III. DATA PRIVACY PRINCIPLES

Processing of Personal Data within in possession of BMC should be undertaken, in compliance with the principles under the DPA, namely:

a. *Transparency* - Data Subject must be aware of the nature, purpose, and extent of the processing of his or her Personal Data by BMC, 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.

b. *Legitimate purpose* - Processing of Personal Data by BMC shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

c. *Proportionality* - Processing of Personal Data shall be adequate, relevant, suitable, necessary, and not excessive, in relation to a declared and specified purpose. Personal Data shall be processed by BMC only if the purpose of the Processing could not reasonably be fulfilled by other means.

IV. DATA PROTECTION OFFICER

A Data Protection Officer **("DPO")** shall be appointed by BMC. The DPO shall be responsible for ensuring compliance with this Policy as well as the applicable laws and regulations for the protection of data privacy and security. The duties and responsibilities of the DPO shall be, among others:

a. Monitor BMC's Personal Data processing activities to ensure compliance with this Policy, including the applicable data privacy laws and regulations;

b. Conduct internal audits and review to ensure that this Policy is strictly observed by all BMC employees and its authorized agents or PIPs;

c. Liaise between BMC and regulatory and accrediting bodies, for purposes of registration, notification, and reportorial requirements under the DPA and other applicable data privacy laws and regulations;

d. Develop, establish, and review the policies and procedures related to the exercise by Data Subjects of their rights under the DPA and other applicable laws and regulations on data privacy;

e. Act as primary point of contact whom Data Subject may coordinate and consult with regarding concerns on their Personal Data;

f. Develop capacity building, orientation, and training programs for employees, agents or representatives of BMC regarding Personal Data privacy and security policies;

g. Prepare and file annual report of the summary of documented security incidents and Personal Data breaches, if any, as required under the DPA and other issuances of the Commission.

V. RIGHTS OF THE DATA SUBJECT

A Data Subject has the following rights:

TO BE INFORMED

1. Data Subject has a right to be informed whether Personal Data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.

2. Data Subject shall be notified and furnished, before the entry of his or her Personal Data into the processing system of BMC, or at the next practical opportunity, with the following information:

    a. Description of the Personal Data to be entered into the system;

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

    c. Basis of processing, when processing is not based on the consent of the Data Subject;

    d. Scope and method of the Personal Data processing;

    e. The recipients or classes of recipients to whom the Personal Data are or may be disclosed;

    f. 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;

g. The identity and contact details of the Personal Data controller or its representative;

h. The period for which the information will be stored; and

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

TO OBJECT

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. 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.

In the event that a Data Subject objects or withholds consent, the PIC shall no longer process the Personal Data, unless:

1. It is needed pursuant to a subpoena;

2. Its collection and processing are 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 collector and the Data Subject; or

3. It is being collected and processed as a result of a legal obligation.

ACCESSIBILITY

Data Subject, upon demand, has the right to the following:

1. Contents of his or her Personal Data that were processed;

2. Sources from which Personal Data were obtained;

3. Names and addresses of recipients of the Personal Data;

4. Manner by which such data were processed;

5. Reasons for the disclosure of the personal data to recipients, if any;

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

7. Date when his or her personal data concerning the Data Subject were last accessed and modified; and

8. The designation, name or identity, and address of the PIC.

TO RECTIFY

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

TO ERASE OR BLOCK

Data Subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her Personal Data from the PIC's filing system.

1. This right may be exercised upon discovery and substantial proof of any of the following:

   (a) The Personal Data is incomplete, outdated, false, or unlawfully obtained;

   (b) The Personal Data is being used for purpose not authorized by the Data Subject;

   (c) The Personal Data is no longer necessary for the purposes for which they were collected;

   (d) The Data Subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;

   (e) 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;

   (f) The processing is unlawful;

   (g) The PIC or PIP violated the rights of the Data Subject.

2. The PIC may notify third parties who have previously received such processed personal information.

DAMAGES

Data Subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of Personal Data, taking into account any violation of his or her rights and freedoms as such.

TRANSMISSIBILITY OF RIGHTS

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 in case of incapacity or inability to exercise the rights as enumerated under this Policy.

DATA PORTABILITY

Where Data Subject's Personal Data is processed by electronic means and in a structured and commonly used format, the Data Subject shall have the right to obtain from the PIC 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 Commission may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

VI. LIMITATIONS

The immediately preceding clause shall not be applicable if the processed Personal Data are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the Data Subject, provided, that the Personal Data shall be held under strict confidentiality and shall be used only for the declared purpose. It is also not applicable to the processing of Personal Data gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of Data Subject. Any limitations on the rights of the Data Subject shall only be to the minimum extent necessary to achieve the purpose of said research or investigation.

VII. DATA COLLECTION PROCEDURES

The DPO, with the assistance of Division HR and any other departments of the Company responsible for the Processing of Personal Data, shall document the Company's Personal Data Processing 6 procedures. The DPO shall ensure that such procedures are updated and that the consent of the Data Subjects (when required by the DPA or other applicable laws or regulations) is properly obtained and evidenced by written, electronic or recorded means. Such procedures 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.

VIII. PROCESSING OF PERSONAL DATA

Consistent with the data privacy principles under the DPA, Personal Data must be:

a. Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

b. Processed fairly and lawfully;

c. Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal data, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;

d. Adequate and not excessive in relation to the purposes for which they are collected and processed;

e. Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and

f. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed, provided, that 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 further, that adequate safeguards are guaranteed by said laws authorizing their processing.

PERSONAL INFORMATION

Processing of Personal Information shall undertake only for a just or lawful purpose and when at least one of the following conditions exists:

a. The Data Subject has given his or her consent;

b. The processing of Personal Data is necessary and is related to the fulfillment of a contract with the Data Subject or in order to take steps at the request of the Data Subject prior to entering into a contract;

c. The processing is necessary for compliance with a legal obligation to which the PIC is subject;

d. The processing is necessary to protect vitally important interests of the Data Subject, including life and health;

e. The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of Personal Data for the fulfillment of its mandate; or

f. The processing is necessary for the purposes of the legitimate interests pursued by the PIC or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the Data Subject which require protection under the Philippine Constitution.

SENSITIVE AND PRIVILEGED INFORMATION

Processing of Sensitive and Privileged Information is prohibited, except in any of the following cases:

a. Consent is given by Data Subject, or by the parties to the exchange of Privileged Information, prior to the processing of the Sensitive Information or Privileged Information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose;

b. The processing of the Sensitive Information or Privileged Information is provided for by existing laws and regulations, unless said laws and regulations do not require the consent of the Data Subject for the processing, and guarantee the protection of personal data;

c. The processing is necessary to protect the life and health of the Data Subject or another person, and the Data Subject is not legally or physically able to express his or her consent prior to the processing;

d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations provided that:

    1. Processing is confined and related to the bona fide members of these organizations or their associations;

    2. The Sensitive Information are not transferred to third parties; and
    3. Consent of the Data Subject was obtained prior to processing;

e. The processing is necessary for the purpose of medical treatment, provided, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured; or

f. The processing concerns Sensitive Information or Privileged Information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

DPO may invoke the principle of privileged communication over Privileged Information that the PIC lawfully controls or processes. Subject to existing laws and regulations, any evidence gathered from Privileged Information is inadmissible.

When the Commission inquires upon communication claimed to be privileged, the DPO shall prove the nature of the communication in an executive session. Should the communication be determined as privileged, it shall be excluded from evidence, and its contents thereof shall not form part of the records of the case, provided, that where the privileged communication itself is the subject of a breach, or a privacy concern or investigation, it may be disclosed to the Commission but only to the extent necessary for the purpose of investigation, without including its contents in the records.

IX. DATA RETENTION SCHEDULE

Subject to applicable requirements of the DPA and other relevant laws and regulations, Personal Data shall not be retained by BMC for a period longer than necessary and/or proportionate to the purposes for which such data was collected. The DPO, with the assistance of the PIC and any other departments of BMC 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.

X. DATA BREACH

NOTIFICATION

a. The DPO and affected Data Subjects shall be notified by the PIC within an hour upon discovery or knowledge of the breach.

b. The DPO must notify the Commission, within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the PIC or PIP that, a Personal Data breach requiring notification has occurred.

b. Notification of Personal Data breach shall be required when Sensitive Information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the PIC or the DPO believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected Data Subject.

c. Depending on the nature of the incident, or if there is delay or failure to notify, the DPO may investigate the circumstances surrounding the Personal Data breach. Investigations may include on-site examination of systems and procedures.

CONTENTS

The notification shall at least describe the nature of the breach, the Personal Data possibly involved, and the measures taken by the entity to address the breach. The notification shall also include immediate measures taken to reduce the harm or negative consequences of the breach, the representatives of the PIC, if any, including their contact details, from whom the Data Subject can obtain additional information about the breach, and any assistance to be provided to the affected Data Subjects.

DELAY

Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

In evaluating if notification is unwarranted, the DPO may take into account compliance by the PIC with this Policy and existence of good faith in the acquisition of Personal Data.

The DPO may exempt a PIC from notification where, based on reasonable judgment, such notification would not be in the public interest, or in the interest of the affected Data Subjects.

The DPO may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

BREACH REPORT

The PIC shall notify the DPO by submitting a report, whether written or electronic, containing the required contents of notification within the period required under this Policy. The report shall also include the name of a designated representative of the PIC, and his or her contact details.

All security incidents and Personal Data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of Personal Data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the PIC or DPO. In other security incidents not involving Personal Data, a report containing aggregated data shall constitute sufficient documentation.

These reports shall be made available when requested by the Commission. A general summary of the reports shall be submitted to the Commission annually.

XI. SECURITY MEASURES

BMC shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of Personal Data it collected or received from Data Subjects.
The DPO shall take steps to ensure that any employee of BMC acting under the PIC's authority and who has access to Personal Data, does not process them except upon the PIC's instructions, or as required by law.

The security measures shall aim to maintain the availability, integrity, and confidentiality of Personal Data and are intended for the protection of Personal Data against accidental or unlawful destruction, alteration, and disclosure, including other forms of unlawful processing. These measures shall be implemented by BMC to protect 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.

PHYSICAL SECURITY MEASURES

BMC will ensure strict compliance with the following guidelines for physical security:

a. 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;
b. Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing Personal Data, taking into consideration the environment and accessibility to the public;

c. The duties, responsibilities and schedule 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;

d. Any department involved in the processing of Personal Data shall implement policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of Personal Data; and

e. Policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and workstation 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.

TECHNICAL SECURITY MEASURES

BMC will ensure strict compliance with the following guidelines for physical security:

a. A security policy with respect to the processing of Personal Data;

b. Safeguards to protect their computer network 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 through an electronic network;

c. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

d. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a Personal Data breach;

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

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

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

LEVEL OF SECURITY

To determine the appropriate level of security, the DPO shall take into account the nature of the personal data that requires protection, the risks posed by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation. The security measures provided herein shall be subject to regular review and evaluation, and may be updated as necessary by the Commission in separate issuances, taking into account the most appropriate standard recognized by the information and communications technology industry and data privacy best practices

XII. DATA SHARING

Processing of Personal Data collected by BMC from a party other than the Data Subject shall be allowed under any of the following conditions:

a. Data sharing shall be allowed when it is expressly authorized by law, provided, that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose and proportionality.

b. Data Sharing shall be allowed if the Data Subject consents to data sharing, and the following conditions are complied with:

1. Consent for data sharing shall be required even when the data is to be shared with an affiliate or mother company, or similar relationships;

2. Data sharing for business or commercial purposes, including direct marketing, shall be covered by a data sharing agreement.

    i. The data sharing agreement shall establish adequate safeguards for data privacy and security, and uphold rights of Data Subjects.

    ii. The data sharing agreement shall be subject to review by the DPO.

3. The Data Subject shall be provided with the following information prior to collection or before data is shared:

    i. Identity of the PIC or PIP that will be given access to the Personal Data;

    ii. Purpose of data sharing;

    iii. Categories of Personal Data concerned;

    iv. Intended recipients or categories of recipients of the Personal Data;

    v. Existence of the rights of Data Subjects, including the right to access and correction, and the right to object;

    vi. Other information that would sufficiently notify the Data Subject of the nature and extent of data sharing and the manner of processing.

4. Further processing of shared data shall adhere to the data privacy principles laid down in this Policy, including the DPA and other rules, and issuances of issued by the Commission.

c. Data collected from parties other than the Data Subject for purpose of research shall be allowed when the Personal Data is publicly available, or has the consent of the Data Subject for purpose of research, provided, that 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. The rights of the Data Subject shall be upheld without compromising research integrity.

XIII. MANAGEMENT OF HUMAN RESOURCES

BMC shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data.

Said employees, agents, or representatives shall operate and hold Personal Data under strict confidentiality if the Personal Data are not intended for public disclosure. This obligation shall continue even after leaving the public service, transferring to another position, or upon terminating their employment or contractual relations. Capacity building, orientation or training programs shall be developed and implemented for such employees, agents or representatives, regarding privacy or security policies.

XIV. SUBCONTRACTING AND OUTSOURCING

BMC may subcontract or outsource the processing of Personal Data, provided, that the it shall utilize contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the Personal Data processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Policy, the DPA and applicable rules related to processing of Personal Data, including issuances of the Commission.

Processing by a PIC shall be subject to a contract or other legal act that binds the PIP to BMC.

The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of Data Subjects, the obligations and rights of the PIP, and the geographic location of the processing under the subcontracting agreement, including a stipulations that the PIP shall:

1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;

2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data;

3. Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission;

4. Not engage another processor without prior instruction from the personal information controller: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;

5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;

6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account

the nature of processing and the information available to the personal information processor;

7. At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the Act or another law;

8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter; and

9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission.

The PIP shall comply with the requirements of this Policy, the DPA and applicable rules related to processing of Personal Data, including issuances of the Commission, in addition to obligations provided in a contract, or other legal act with BMC.

XV. PENALTIES

Violation of this Policy shall be considered a valid ground for termination and any employee who, based on substantial evidenced and after notice and hearing, has been found to have committed such violation shall be immediately dismissed from employment, without prejudice to the right of BMC to be compensated for any loss or damage that it might have suffered by reason of the violation committed by the guilty employee, including the right the file a criminal case, if warranted.