DMCI HOLDINGS INCORPORATED	Classification: Corporate Policy	Document No. DPM2018-0001
	Document Title: **DATA PRIVACY MANUAL**	Date: March 20, 2018 Page: 1 of 45

Contents

Revision History

Issue No.	Date	Description of Change	Approved
	03-20-2018	Newly established policy	

1.0 INTRODUCTION

1.1 DMCI Holdings, Inc. ("DMCIHI" or "the Company") endeavors to meet leading standards and regulations for data protection and privacy. The Company respects and values data privacy rights, and makes sure that all personal data collected from the data subjects are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality. While our reasons are founded in ethical and corporate responsibility, our privacy practices as outlined in this policy facilitate the following:

- *Good Corporate Citizenship:* A sound Privacy Policy is emblematic of reliable corporate citizens that respect data subjects' privacy.
- *Business Enablement:* Since DMCIHI uses significant volumes of personal data, Privacy Policy become a prerequisite to building enduring business relationships.
- *Legal Protection:* Appropriate privacy policies offer an opportunity to eliminate allegations of unlawful usage of personal information.

1.2 The policies and guidelines stated on this Data Privacy Manual (or simply "Manual") are based on the requirements of Republic Act Number 10173, also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulation (IRR) and other relevant policies, including issuances of the National Privacy Commission ("NPC" or "the Commission").

1.3 This Manual shall inform the data subjects of the Company's data protection and security measures, and may serve as their guide in exercising their rights under the DPA.

2.0 OBJECTIVE(S)

2.1. To make sure the Company manage personal information in an open and transparent way.

2.2. To ensure that all of the personal data in DMCIHI's custody is adequately protected against threats to maintain its security.

2.3. To ensure that the Company's employees are fully aware of the contractual, statutory or regulatory implications of any privacy breaches.

2.4. To limit the use of personal data to identified business purposes for which it is collected.

2.5. To create an awareness of privacy requirements to be an integral part of the day to day operation of every employee and ensure that all employees understand the importance of privacy practices and their responsibilities for maintaining privacy.

2.6. To make all the employees aware about, the processes that need to be followed for collection, lawful usage, disclosure/ transfer, retention, archival and disposal of personal data.

2.7. To ensure that all third parties collecting, storing and processing personal data on behalf of the Company provide adequate data protection.

2.8. To ensure that applicable regulations and contracts regarding the maintenance of privacy, protection and cross border transfer of personal data are adhered to.

2.9. To provide the Company with guidelines to follow in respect of privacy, which are in accordance with Philippine Data Privacy Act of 2012 (DPA) and other applicable data privacy laws.

2.10. To help ensure compliance with laws and regulations applicable to DMCIHI's collection, storage, use, transmission, disclosure to third parties and retention of personal and sensitive personal data information.

3.0 SCOPE AND LIMITATIONS

3.1 This Manual is applicable to **all** DMCIHI's management, employees, contractors, vendors, interns, customers, shareholders, investors and agents who may receive personal data from DMCIHI, or who provide information to DMCIHI. It covers personal data collected or processed by or on behalf of DMCIHI including its Personal Information Processor/s (PIP/s).

3.2 This Manual covers the treatment of personal information gathered and used by DMCIHI for lawful business purposes. This policy also covers the personal information shared with authorized Third Parties or that Third Parties shared with DMCIHI.

3.3 Any requests for exceptions to this policy should firstly be referred to the DPO. Written approval from the DPO should then be forwarded to the person requesting the exception.

4.0 DEFINITION OF TERMS

4.1 **Access -** refers to an individual's right to see and know about his or her own personal data that the Company holds.

4.2 **Anonymize –** to process a collection of personal data or information such that a natural person cannot be identified on the basis of the output collection of data or information.

4.3 **Collection** – refers to the process of gathering, acquiring or obtaining personal information from any source, by any means, in circumstances where the individual is identified or is reasonably identifiable. It includes information that:

- is publicly available information about an identifiable individual that the Company comes across;
- information the Company receives directly from the individual; and
- information about an individual the Company receives from somebody else.

4.4 **Company –** refers to DMCI Holdings, Inc. ("DMCIHI")

4.5 **Compliance Officer for Privacy (COP)** - Refers to an individual that performs some of the functions of a DPO, as provided in NPC Advisory No. 17-01

4.6 **Data Privacy Act of 2012 or DPA** – refers to Republic Act No. 10173 or the Philippine Data Privacy Act of 2012 and its implementing rules and regulations (IRR).

4.7 **Data Privacy Manual ("Manual")** - establish policies, and implements measures and procedures that guarantee the safety and security of personal data under the Company's control or custody, thereby upholding an individual's data privacy rights.

4.8 **Data Protection Officer (DPO)** – refers to the individual designated by the DMCIHI to be accountable for its compliance with the Act, its IRR, and other issuances of the Commission: provided, that, except where allowed otherwise by Law or the Commission, the individual must be an organic employee of DMCIHI: provided further, that DMCIHI may have more than one DPO.

4.9 **Data Processing Systems** – refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.

4.10 **Data Sharing –** is the disclosure or transfer to a third party of personal data under the custody of a personal information controller (PIC) or personal information processor (PIP). In the case of the latter, such disclosure or transfer must have been upon the instructions of the PIC concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a PIC to a PIP.

4.11 **Data Sharing Agreement –** a contract, joint issuance, or any similar document that contains terms and conditions of a data sharing agreement between two or more parties provided that only PICs shall be made parties to a data sharing agreement.

4.12 **Data Subject –** refers to a living individual whose personal information, sensitive personal information, or privileged information is processed by or on behalf of the Company.

4.13 **Data Subject Information Request –** any request received by the Company from a Data Subject or other individual or legal entity who wishes to receive a copy of all the Personal Data related to it or him the Company is processing about it or him.

4.14 **Direct Marketing –** refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals, which includes activities that promote the sale or purchase of products or services or promote charitable fundraising where the individual is approached directly. It includes in-person approaches to people's houses and approaches by mail, e-mail, facsimile and phone. It includes individually targeted approaches by these means where people are encouraged to buy services at a distance (for example, to buy by phone, mail or website) or to visit retail and service outlets or to donate to a cause by one of these means.

4.15 **Disclosure –** means rendering personal data accessible, for example by allowing access to personal data either transferring, distributing, or publishing the personal data.

4.16 **Personal Data –** collectively refers to personal information, sensitive personal information, and privileged information.

4.17 **Personal Data Breach (or simply "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. It occurs also when an unauthorized party

acquires the personal data of a client, agent, or employee without it being adequately secured or encrypted.

4.18 **Personal Data Lifecycle -** is composed of collection, usage, access and correction, disclosure and distribution/data sharing, storage and transmission, retention, and disposal and destruction.

4.19 **Personal Data Processing System** - refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.

4.20 **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.

4.21 **Personal Information Controller (PIC) –** refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

- A natural or juridical person, or any other body, who performs such
- functions as instructed by another person or organization; or
- A natural person who processes personal data in connection with his or her personal, family, or household affairs.

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.

4.22 **Personal Information Processor (PIP) –** 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.

4.23 **Primary Purpose** – is the dominant or fundamental reason for information being collected in a particular transaction. There can only be one primary purpose of collection for a particular transaction. When an individual gives (and the Company collects) personal information, the individual and the Company almost always do so for a particular purpose, for example, to buy or sell a particular product or to receive a service. This is the primary purpose of collection, even if the Company has some additional purposes in mind. These additional purposes will always be secondary purposes for that transaction, even if the Company tells the person about them, and even if the Company obtains the individual's consent to use or disclose the information for those additional purposes.

4.24 **Privacy Impact Assessment (PIA)** – a process undertaken and used to evaluate and manage the impact on privacy of a particular project, program, process or measure.

4.25 **Privileged Information –** refers to any and all forms of Personal Data, which, under the Rules of Court and other pertinent laws constitute privileged communication.

4.26 **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.

4.27 **Profiling** - Any form of automated processing of personal data consisting of the use of personal data, such as an individual's economic situation, political or religious beliefs, behavioral or marketing activities, personal

preferences, electronic communication data, location data, and financial data, among others, in order to evaluate, analyze, or predict his or her performance, qualities, and behavior, among others.

4.28 **Reasonable** – Generally speaking, they relate to decisions or steps to be taken by the Company in particular circumstances (for example, when collecting, correcting or using and disclosing information) or to expectations of individuals in those circumstances. Determining what is reasonable involves considering the factual circumstances in which a person or organization is acting rather than the individual's or organization's view of what is reasonable or unreasonable.

4.29 **Related Purpose** – includes all the purposes that are directly related purposes as well as certain additional ones. Related purposes must have some connection to, and arise in the context of, the primary purpose. Uses or disclosures for a related purpose would include uses or disclosures:

- giving a person information closely associated with a particular product or service a person receives from the Company; or
- notifying a person who has received a service or product from the Company in the past of a business change of address.

4.30 **Required by Law** - refers to circumstances where a law (other than the Data Privacy Act of 2012) requires the Company to collect, use or disclose or deny access to, personal information. In certain instances, failing to comply with such a legal requirement may be an offence. Such a law may specifically require the Company to collect, use, disclose or deny access. It may also be a law that gives another body, such as a government agency, a general information gathering power that includes the power to require the Company to disclose information to it.

4.31 **Security Incident –** is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of Personal Data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.

4.32 **Sensitive Personal Information/ Sensitive Personal Data** – refers to personal information:

4.32.1 The Data Privacy Act of 2012, Philippines:

- about an individual's race, ethnic origin, marital status, age, color and religious, philosophical or political affiliations;
- about an individual's health, education, genetic or sexual life of a person, 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;
- about an individual's personal contact details, and home address;
- 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 it denials, suspension or revocation and tax returns; and
- specifically established by an executive order or an act of Congress to be kept classified.

4.33 **Third Party –** All external parties – including without limitation contractors, interns, agents, vendors, service providers and partners – who have access to the Company's information assets, information systems or who are pass personal information from them.

4.34 **Unsolicited Personal Information –** refers to personal information received by the Company where the Company has taken no active steps to collect the information.

4.35 **Use** – relates to the handling of the personal information within the Company. Examples of uses of information are:

- adding information to a database;
- forming an opinion based on information collected and noting it on a file; and
- including information in a publication.

5.0 REFERENCES (POLICY/PROCEDURES)

5.1. **Applicable Privacy Law:** The Philippine Data Privacy Act of 2012 (DPA) is a 21st century law to address 21st century crimes and concerns. It (1) protects the privacy of individuals while ensuring the free flow of information to promote innovation and growth; (2) regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure and destruction of personal data; and (3) ensures that the Philippines complies with international standards set for data protection through the National Privacy Commission (NPC). This covers the Implementing Rules and Regulations (IRR) of DPA with respect to data protection, issuances by the NPC and other applicable laws and policies.

5.2. **Relevant Company Policies and Procedures:**
xx-xx-001, Data Incident Notification Protocol

xx-xx-002, Information Security Policy

xx-xx-003, Data Privacy Training Materials

6.0 RESPONSIBILITY AND AUTHORITY

6.1 The **Board of Directors (BOD)** shall be responsible to oversee the implementation of this Policy. Any breach of material value, shall be reported to the BOD.

6.2 The **President** shall be responsible to channel resources and address organizational issues related to privacy.

In the event the position of DPO or COP is left vacant, the President should provide for the appointment, reappointment, or hiring of his or her replacement within a reasonable period of time. The President may

also require the incumbent DPO or COP to occupy such position in a holdover capacity until the appointment or hiring of a new DPO or COP, in accordance with the Company's internal policies or the provisions of the appropriate contract.

6.3 The **Data Protection Officer (DPO)** shall act as a central authority for the implementation and enforcement of Company's Data Privacy Program. The DPO is required to advocate for the privacy program, articulate and communicate the Company's privacy goals, and lead enforcement of the Data Privacy Policy. To achieve this, the appointed DPO should have the organizational credibility to facilitate decision making and resource allocation.

6.3.1 A DPO shall be appointed by the Company, through its BOD/President.

Qualifications:

6.3.2 The DPO should possess specialized knowledge and demonstrate reliability necessary for the performance of his or her duties and responsibilities. As such, the DPO should have expertise in relevant privacy or data protection policies and practices.

6.3.3 He or she should have sufficient understanding of the processing operations being carried out by the Company or its PIP/s, including the latter's information systems, data security and/or data protection needs.

6.3.4 Knowledge by the DPO of the sector or field of the PIC or PIP, and the latter's internal structure, policies, and processes is also useful.

6.3.5 The DPO or COP should be a full-time or organic employee of the Company or PIP.

6.3.6 The DPO or COP should ideally be a regular or permanent position (consultants and project, seasonal, probationary, or casual employees should not be designated as DPOs). Where the employment of the DPO or COP is based on a contract, the term or duration thereof should at least be two (2) years to ensure stability.

6.3.7 A DPO or COP must be independent in the performance of his or her functions, and should be accorded a significant degree of autonomy by the PIC or PIP.

6.3.8 In his or her capacity as DPO or COP, an individual may perform (or be assigned to perform) other tasks or assume other functions (e.g., legal counsel, risk management officer, etc.) that do not give rise to any conflict of interest.

The minimum qualifications for a Privacy Coordinator/COP shall be proportionate to his or her functions, as provided in NPC's Advisory.

6.4 The **Privacy Coordinator (PC)** is an individual or individuals who shall perform some of the functions of a DPO shall act as advocates for the Data Privacy Program in their respective departments and locations. Situating the responsibility for the data privacy program locally and across the Company enables optimal resource placement and organizational awareness.

6.4.1 A Privacy Coordinator shall be appointed or designated by the Company for each department of the Parent Company and a COP shall be appointed or designated by the Company where the Company has subsidiaries, sub-offices, or any other component units.

6.4.2 Generally, a Privacy Coordinator/COP has the same duties and responsibilities with DPO, however the scope of the former covers only the branch, sub-office or component unit under his or her responsibility.

6.5 The Company may outsource or subcontract the functions of its DPO or Privacy Coordinator/COP. However, to the extent possible, the DPO or Privacy Coordinator/COP must oversee the performance of his or her functions by the third-party service provider or providers. The DPO shall also remain the contact person of the PIC or PIP vis-à-vis the NPC.

6.6 To strengthen the autonomy of the DPO or Privacy Coordinator/COP and ensure the independent nature of his or her role in the Company, a PIC or PIP should not directly or indirectly penalize or dismiss the DPO or Privacy Coordinator/COP for performing his or her tasks. It is not necessary that the penalty is actually imposed or meted out. A mere threat is sufficient if it has the effect of impeding or preventing the DPO or Privacy Coordinator/COP from performing his or her tasks. However, nothing shall preclude the legitimate application of labor, administrative, civil or criminal laws against the DPO or Privacy Coordinator/COP, based on just or authorized grounds.

For an illustrative diagram of the privacy organizational structure and detailed discussion of the key obligations of responsible parties above, please refer to **Appendix 1**.

7.0 DATA PRIVACY POLICIES

7.1 Data Privacy Principles

7.1.1 All processing of personal data within the Company shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.

7.1.1.1 ***Transparency.*** The data subject must be aware of the nature, purpose, and extent of the Processing of his or her personal data by the Company, 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.

7.1.1.2 ***Legitimate Purpose.*** The processing of personal data by the Company shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

7.1.1.3 ***Proportionality.*** The 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 the Company only if the purpose of the processing could not reasonably be fulfilled by other means.

7.2 Guidelines for the Processing of Personal Data

7.2.1 Collection

7.2.1.1 Collection of Sensitive Personal Information

1. Employees, authorized agents and brokers must only collect sensitive personal information:
   - Where the information is reasonably necessary for one or more of the Company's functions *(Employee's 201 File and others like it)* or activities and with the individual's consent (Refer to DMCIHI Suggested Wordings Consent Form for the suggested wordings for a consent form); or
   - If the collection is required by law *(i.e. Bureau of Internal Revenue, Social Security System, Philippine Health Insurance Corporation, Home Development Mutual Fund, among others)*
2. Should collection of sensitive personal information of an individual is reasonable necessary, employees, authorized agents and brokers must take reasonable steps to ensure that the individual is aware of the matters listed under **7.2.1.2 Collection of Personal Information**.

7.2.1.2 Collection of Personal Information

1. Employees must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the Company's functions or activities. Collection of personal information must only through lawful and fair means. Should collection of personal information of an individual is reasonably necessary, employees must take reasonable steps to ensure that the individual is aware of the following:
   - The identity and contact details of DMCIHI as the Company collecting and storing the information;
   - The fact that he or she is able to gain access to the information and seek correction;
   - The purpose for which the information is collected;
   - The extent of processing, including, where applicable, the automated processing of his or her personal data for profiling;
   - The intended recipients or third parties to which the Company usually discloses information of that kind, including any overseas recipients and the countries in which those recipients or third parties or entities and the countries in which those recipients are likely to be located;
   - The fact that he or she may make a privacy complaint and how the Company will deal with it;
   - Any law that requires the particular information to be collected;
   - The main consequences, if any, for an individual if all or part of the information is not provided; and
   - The period of retention of his or her personal information after processing.
2. Where is it reasonable and practical to do so, employees, authorized agents and brokers will only collect personal information from the individual alone. Should personal information are collected from an individual other than the data subject, employees, authorized agents and

brokers must act reasonably to ensure that the data subject is or has been made aware of the matters listed above.

7.2.1.3 **Receiving Unsolicited Personal Data.** Where employees, authorized agents and brokers receive unsolicited personal data about an individual they must determine within a reasonable time whether they could have collected the information in accordance with **7.2.1.1 Collection of Sensitive Personal Information** and **7.2.1.2 Collection of Personal Information**. Should the Collection is not in accordance to the sections above, the employees, authorized agents and brokers, only if it is lawful and reasonable, shall inform the data ssubject that the data being given is not needed and must soon as practical either destroy or de-identify the personal information.

7.2.1.4 **Collection of Personal Data for Research.** Employees, authorized agents and brokers may collect personal data of an individual for research from a party or parties other than the data subject when:

1. The personal data is publicly available; or
2. 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.

7.2.2 **Storage**

7.2.2.1 All employees, authorized agents and broker who store personal data on paper, film, optical or magnetic media either on-site or off-site must:

1. Exercise due diligence for keeping the data safe and secure; and

2. Integrate organizational, technical and physical security measures.

7.2.3 Usage, Disclosure and Sharing

7.2.3.1 As a general rule, employees, authorized agents and brokers must not use personal data of a data subject other than for its primary purpose of collection, unless:

1. The data subject has consented to the use or disclosure; or
2. The data subject would reasonably expect the Company to use or disclose non-sensitive personal information for a secondary purpose and the secondary purpose is related to the primary purpose; or
3. The Company has reason to suspect that unlawful activity has been, or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
4. The use or disclosure is required under a law, or by a regulation; or
5. The Company reasonably believes that the use is reasonably necessary for a specified purpose by or on behalf of an enforcement body; or
6. The use or disclosure is required or authorized by or under law or contract with third parties covered by a data sharing agreement (for the suggested wording to be included in the General Terms and Conditions for a DMCIHI standard contract, refer to **Appendix 2**; for the normative data sharing template, refer to DMCIHI Data Sharing Agreement Template and DMCIHI Outsourcing Agreement Template); or
7. The Company reasonably believes the use is necessary to prevent or lessen a serious and imminent threat to

public health or public safety or the life or health of an individual; or

7.2.3.2 *Provided*, that further processing of shared data shall adhere to the **7.1. Data Privacy Principles** and applicable privacy laws and regulations.

7.2.3.3 ***Cross-border Data Flows***

1. Any form of sharing personal data to an organization or individual out the Philippines should be allowed only if:
   - The data subject has consented to the transfer; or
   - The organization reasonably believes that the recipient is subject to laws or a contract enforcing information handling principles substantially similar to applicable privacy laws in the Philippines (i.e. DPA); or
   - The transfer is necessary for the performance of a contract between the individual and the organization; or
   - The transfer is necessary as part of a contract in the interest of the data subject between the organization and a third party; or
   - The transfer is for the benefit of the data subject; or
   - It is impractical to obtain the consent of the data subject; or
   - If it were practicable the data subject would likely consent.
2. *Provided*, that the organization will take reasonable steps so that the information transferred will be held, used and disclosed consistently with the applicable privacy laws in the Philippines (i.e., DPA).

7.2.4 **Access and Correction**

7.2.4.1 As a general rule, the Company's DPO will, upon written request or demand, provide the data subject with access to

his or her personal data within a reasonable time after such written request or demand is made, as well as to immediately address a request for correction of his or her personal data.

7.2.4.2 The Company's DPO cannot impose a charge upon the data subject to cover the cost of locating, retrieving, reviewing and copying any material requested by him or her.

7.2.4.3 The Company's DPO may however choose not to provide an individual with access to such information. If giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety.

Then in such cases the Company's DPO will give the individual a written notice that sets out:

- The reasons for the refusal where it is reasonable to do so; and
- The way in which the individual may make a complaint about such refusal.

7.2.4.4 ***Maintaining Data Quality.*** Employees must take reasonable steps to:

a. Assure that personal data of the data subjects collected, used or disclosed are accurate, complete, kept up to date and not misleading; and
b. Rectify, supplement, destroy, or further process inaccurate or incomplete data.

7.2.5 Retention

7.2.5.1 Personal data of the data subjects collected, used and disclosed by the Company shall only be retained:

1. For the fulfilment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated; or
2. For the establishment, exercise or defense of legal claims; or
3. For the legitimate business purposes, which must be consistent with standards followed by the Company or approved by appropriate government agency; or
4. In any case provided by law.

7.2.5.2 Retention period:

1. For financial data collected, 10 years based on required retention period as mandated by the Philippine laws; or
2. For personnel records collected, two (2) years after termination; or
3. For CCTV recordings, retention of records in the system is for sixty (60) days, in cases where there is breach in security, the company administrative department shall record video coverage such incidents on file for ten (10) years; or
4. In any case provided by law.

7.2.6 Destruction/Disposal

7.2.6.1 All files that contain personal data must be securely disposed, destroyed or permanently de-identify, whether such files are:

1. Stored on paper, film, optical or magnetic media; and
2. Any computer equipment, such as disk servers, desktop computers and mobile phones at end-of-life (especially storage media) provided that the procedure shall include the use of degaussers, erasers, and physical destruction devices;
3. Stored offsite, outsourced, or subcontracted.

7.2.6.2 *Provided*, that the Company has no legitimate reason for retaining such files as provided under **7.2.5 Retention of Personal Data**.

7.3 Security Measures

7.3.1 Organizational Measures

7.3.1.1 Conduct Privacy Impact Assessment

The Company shall conduct a PIA relative to all activities, projects and systems involving the processing of personal data. It may choose to outsource the conduct of PIA to a third party. For the guidelines in completing the PIA Questionnaire template (DMCIHI Privacy Impact Assessment Questionnaire Template), refer to Appendix 3.

7.3.1.2 *Set up Data Privacy Team*. For a more detailed discussion, refer to Section 6.0 Responsibility and Authority and Appendix 1 for the organizational structure and roles and responsibilities of the Data Privacy Team.

7.3.1.3 Conduct trainings or seminars to keep personnel, especially the Data Privacy Team updated vis-à-vis developments in data privacy and security landscape.

7.3.1.4 Record and document activities carried out by the Data Privacy Team, or the Company itself, to ensure compliance with the DPA, its IRR and other relevant policies.

7.3.1.5 *Duty of Confidentiality.* All employees, contractors and brokers will be ask to sign a Non-Disclosure Agreement. All employees with access to personal data shall operate

and hold personal data under strict confidentiality if the same is not intended for public disclosure.

7.3.1.6 *Review of Manual.* This policy will be reviewed at least every year from its issue date or earlier if deemed required by either of the DPO. All policy changes should be drafted by the DPO and approved by the President/BOD.

7.3.1.7 *Compliance Monitoring and Reporting.* Non-compliance with this Manual may result in a breach of the Data Privacy Policy, the Data Privacy Act of 2012 and other applicable laws.

7.3.2 **Physical Measures**

7.3.2.1 The DPO shall develop and implement policies and procedures for the Company to monitor and limit access to, and activities in, the building property of the Company, including the on-site and off-site offices, areas and workstations of the Company where personal data are collected, used, stored and disposed.

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

7.3.2.3 At the minimum, the following should be part in the policies and procedures:

a. **Format of data collected.** Personal data collection may be in electronic or physical format. Only those systems, websites and paper forms allowed by the Company should be used to collect personal data.
b. **Storage type and location.** All personal data stored by the Company shall be placed in storage rooms with limited access only to selected individuals for paper-

based forms and in filing cabinets with locks for constantly used paper-based forms, and secured server and database rooms in a controlled environment for electronic format.

c. **Access procedure of the Company's personnel.** Strict implementation of access card for every entry and/or exit points in the building. Once terminated, access card should be returned to the Company. Logbooks should be strictly monitored by the guard in-charge for the visitors and guests.

d. **Monitor and limitation of access or facility storage.** Only authorized personnel should be allowed inside the storage area and data center. Borrowing of access cards and keys should not be allowed, unless the requesting employee or visitor will be accompanied by the authorized personnel.

e. **Design of office space or workstation.** Positioning of office space or workstation is encouraged to be arranged with considerable spaces between them to maintain privacy and protect the processing of personal data. Employees should avoid shoulder surfing, eavesdropping and other unauthorized access.

f. **Security perimeters.** Security perimeters should be defined and used to protect areas that contain personal data.

g. **Data Center.** Access to the data center should be limited to only authorized personnel. Environmental controls should be in place as well.

7.3.3 Technical Measures

7.3.3.1 The DPO shall continuously develop and evaluate the Company's security policies and procedures from collection, usage, storage and disposal of personal data.

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

7.3.3.3 At the minimum, the following should be part in the policies and procedures:

a. **Access control.** Access control policy should be monitored and regularly reviewed by the DPO with coordination of IT Department. The policy includes assignments for access management to employees, third parties or contractors; use of multi-factor authentication for use of privileged access and access to any sensitive data; remote access management; and frequency of review of the appropriateness of access of the employees.
b. **Computer system security.** Deploy secure authentication protocols and encryption tool across public networks and wireless connections.
c. **Social media.** Manage and monitor the use and usage of social media accounts of the Company to prevent inadvertent disclosure of information.
d. **Data protection guidelines.** The Company should have data protection guidelines covering data in motion, data at rest, and data in use. Other activities such as create, read, update and delete are logged and actively monitored for appropriateness.
e. **Data leakage protection tool.** Data leakage protection tool should be configured to align with the data classification, data privacy, information security, and

other enterprise policies. The Company should have a process in place to monitor communications, to identify and remediate unencrypted transmission of sensitive information.

f. **Host security.** Formal process to manage anti-virus should be created and monitored based on changing environment as well as tools to be used, and process and frequency for updating definitions. Patch management process should be initiated throughout the change management process and the environment should be reviewed periodically to confirm compliance. Periodic testing, and risk and vulnerability mitigation evaluation should be regularly performed as well.

g. **Software security.** The Company should deploy secure coding, secure configuration, secure development environments, secure production environments, test data definitions and build requirements.

h. **Network security.** The Company should have a process on how the administrative IT credentials are generated, stored and managed; conduct regularly review of network security incidents being identified, logged and followed up; the type of authentication required to access the internal network; and an acceptable use policy and controls that define or restrict what a user can and cannot do on the network.

i. **Vulnerability management.** Use and monitoring of technologies that can identify malware in the environment and process of how the Company performs attack and penetration assessments on its networks and applications.

j. **Third party.** Create a policy governing the use of third party hosting providers; evaluate third party software components for stability, security and overall risk before they are utilized in development projects; Inclusion of security control requirements with the contract with third party.

7.4 **Breach and Security Incidents**

7.4.1 Any suspected or actual personal data breach in whatever form must be reported to immediate manager, Data Breach Response Team or System Incident Response Team (SIRT), and the DPO straight away to enable the appropriate assessment, investigation and remediation measures to be undertaken in a timely manner (including possible notification to local privacy regulators and other relevant bodies). If the breach occurred or is discovered outside normal working hours, notification should be done as soon as practicable. The contact numbers of the SIRT and DPO

7.4.2 The Company's DPO shall notify the Commission within seventy-two (72) hours upon discovery or a reasonable belief that a personal data breach has occurred if and only if, the following are present:

7.4.2.1 There is a breach of sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud;

7.4.2.2 The data is reasonably believed to have been acquired by an unauthorized person; and

7.4.2.3 Either the personal information controller or the NPC believes that the data breach is likely to give rise to a real risk of serious harm to the affected data subject.

7.4.3 If there is doubt as to whether notification is indeed necessary, consider:

7.4.3.1 The likelihood of harm or negative consequences on the affected data subjects;

7.4.3.2 How notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred; and

7.4.3.3 If the data involves:

1. Information that would likely affect national security, public safety, public order, or public health;
2. At least one hundred (100) individuals;
3. Information required by all applicable laws or rules to be confidential; or
4. Personal data of vulnerable groups.

7.4.4 All events must be recorded in the Data Breach Incident Response Tracker (refer to DMCIHI Data Breach Incident Response Tracker).

7.4.5 Initial investigation should be performed by the SIRT as soon as possible within twenty-four (24) hours from the time the personal data breach was reasonably believed to have occurred. Delay may be allowed if the scope of the breach cannot be determined within the 24-hour period. However, the 72-hour period notification to the Commission must be religiously observed.

7.4.6 After notifying NPC, steps shall be taken to notify the affected data subject. Person designated by the PIC shall notify the data subjects individually through a secure means of communication either through written or electronic mail. (refer to DMCIHI Data Breach Notification to NPC and DMCIHI Data Breach Notification to Data Subject).

7.4.7 The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects.

7.4.8 Secured means of individual notifications to affected data subjects must be properly observed either through a written or electronic email.

7.4.9 The Data Breach Response Team must maintain and monitor the Incidents Recording Template, with action items until final resolution.

7.4.10 A general summary of the report shall be submitted by the DPO to the NPC annually in accordance with the requirements of NPC. Refer to DMCIHI Data Breach Summary Report.

7.5 **Inquiries and Complaints**

7.5.1 Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the Company, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the Company at inquiry@dmciholdings.com and briefly discuss the inquiry, together with their contact details for reference.

7.5.2 Complaints shall be filed in three (3) copies, or sent to complaints@dmciholdings.com.

7.5.3 The concerned department or unit shall confirm with the complainant its receipt of the complaint.

8.0 EFFECTIVITY

8.1 The provisions of this Manual are effective this 20 day of March 2018, until revoked or amended by this Company, through a Board Resolution.

9.0 FORMS

7.1 DMCIHI Suggested Wordings Consent Form

7.2 DMCIHI Data Sharing Agreement Template

7.3 DMCIHI Outsourcing Agreement Template

7.4 DMCIHI Privacy Impact Assessment Questionnaire Template

7.5 DMCIHI Data Breach Incident Response Tracker

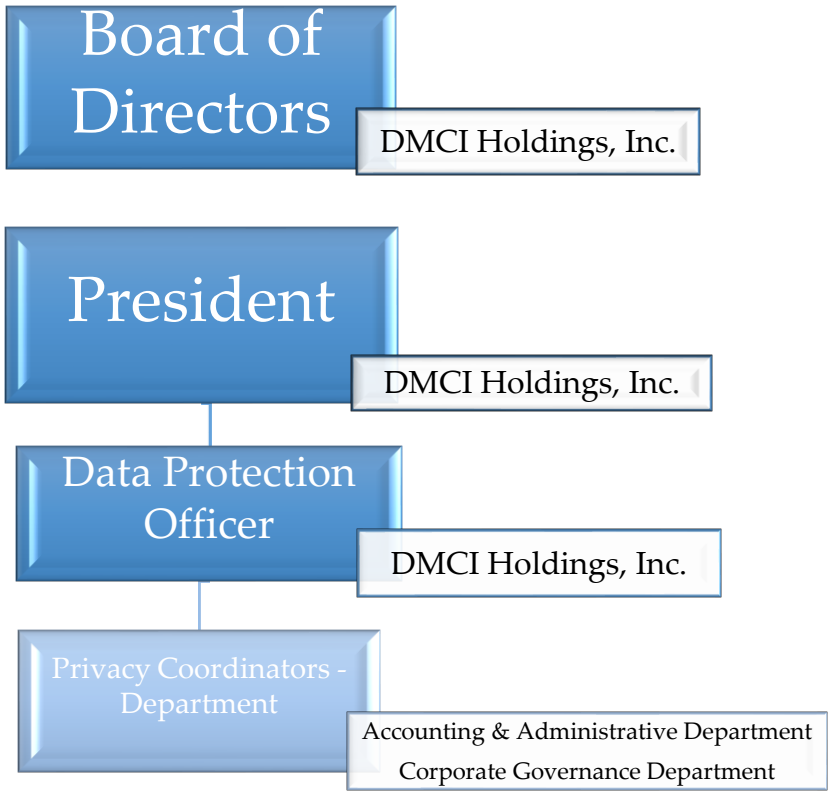
7.6 DMCIHI Data Breach Summary Report

10.0 APPENDICES

Appendix 1 Data Privacy Team

The privacy organization has been designed keeping in mind the various departments and subsidiaries across various business processes where DMCIHI operates. Stakeholders and oversight from key business functions and senior leadership provides sustainable and practical guidance for the privacy framework.

Appendix 1.1 Privacy Organizational Structure


Board of Directors
DMCI Holdings, Inc.
President
DMCI Holdings, Inc.
Data Protection Officer
DMCI Holdings, Inc.
Privacy Coordinators - Department
Accounting & Administrative Department
Corporate Governance Department

Appendix 1.2 Data Privacy Roles and Responsibilities

Responsible Party (*Check applicability*)	**Key Obligations**
Board of Directors (BOD)	• Shall be responsible to oversee the implementation of this Policy. Any breach of material value, shall be reported to the BOD.

President	• Ensure that a Data Protection Officer (DPO)/Compliance Officer for Privacy (COP) is appropriately appointed at all times and effectively communicate his or her functions.
	• Channel resources and address organizational issues related to privacy:
	  o Provide sufficient time and resources (financial, infrastructure, equipment, training, and staff) necessary for the DPO to keep himself or herself updated with the developments in data privacy and security and to carry out his or her tasks effectively and efficiently.
	  o Grant the DPO appropriate access to the personal data it is processing, including the processing systems.
	  o Where applicable, invite the DPO to participate in meetings of senior and middle management to represent the interest of privacy and data protection.
	  o Ensure that the DPO is made a part of all relevant working groups that deal with personal data processing activities conducted inside the Company, or with other organizations.
	• Allow the DPO to be involved from the earliest stage possible in all issues relating to privacy and data protection.
	• Promptly consult the DPO in the event of a personal data breach or security incident.
	• Review and approve the Company's Data Privacy Policy at least on an annual basis.
	• Establish a process for the enforcement of Data Privacy Policy.
	• Ensure the implementation of a Data Privacy Program that enables compliance with the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR) with respect to data

Responsible Party (*Check applicability*)	Key Obligations
	protection, issuances by the National Privacy Commission (NPC) and other applicable laws and policies. • Monitor the Data Privacy Program effectiveness.

Data Protection Officer (DPO)	***Govern***
	• Implement policies, practices, and controls that:
	  o Ensure Company's compliance with applicable privacy laws and privacy principles;
	  o Enable the Company to deal with enquiries or complaints from individuals about the Company's compliance with applicable privacy laws and privacy principles.
	• Develop and maintain a Data Privacy Policy along with the disciplinary and remedial actions for the violation of the Policy.
	• Conduct annual review of the Data Privacy Policy and recommend changes or policy updates to the BOD.
	• Orchestrate the establishment and implementation of a Privacy Management Program, including continuous assessment and revision as regulations and the business environment evolve.
	• Lead and advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of DMCIHI or its PIP/s relating to privacy and data protection measures, by adopting a privacy by design approach.
	• Monitor the DMCIHI and its PIP's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies.
	• Lead the development and conduct of Privacy Impact Assessment (PIA) procedures and ensure its conduct relating to any activities, measures, projects, programs, or systems of DMCIHI or its Personal Information Processor/s (PIP/s), including assistance in the identification, assessment, measurement, and monitoring of risks associated with data privacy for all new projects involving personal data and on any new collection, use or disclosure of personal data.
	• Review PIA submitted by business units.

Responsible Party (*Check applicability*)	Key Obligations
	• Facilitate periodic privacy compliance audits and reviews and present the findings from the periodic privacy compliance reviews and PIA to the BOD to ensure Company's policies, practices, and controls are adequately implemented by its employees. • Develop an oversight and review plan on a periodic basis that sets out how and when the Data Privacy Manual's effectiveness will be monitored and assessed. • Present grievances and information requests along with relevant details to the BOD for exceptions to established response processes. ***Protect*** • Collect information to identify the processing operations, activities, measures, projects, programs, or systems of DMCIHI and its PC's, and maintain a record thereof. • Analyze and check the compliance of processing activities, including the issuance of accreditation and compliance by third-party service providers processing DMCIHI's personal data. • Inform, advice, and issue organizational, technical and physical security recommendations to the DMCIHI and its PC's. • Ascertain renewal of accreditations or certifications necessary, if any, to maintain the required standards in personal data processing. • Advice the DMCIHI or its PC's as regards the necessity of executing a Data Sharing Agreement with third parties and ensure its compliance with the law. ***Educate*** • Inform and cultivate awareness on privacy and data protection within DMCIHI, including all relevant laws, rules and regulations and issuances of the NPC. • Formulate capacity building, orientation, and training programs and provide briefings, information and resources for employees to keep them apprised of current and emerging privacy requirements.

Responsible Party (*Check applicability*)	Key Obligations
	• Provide employees with adequate guidance on identifying and appropriately handling data protection issues that may affect the performance of their job. ***Respond*** • Serve as the contact person for of the PC's vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and DMCIHI or its PC's. • Identify and assess the events that lead to a personal data privacy breach and the impact it could have on the business. • Define, communicate and ensure proper data breach and security incident management by the DMCIHI or its PC's, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period needs to be reported to the affected data subject. • Decide/classify which data breach are required to be reported to regulators, affected individuals and other relevant recipients. • Identify legal issues or requirements that may arise as a result of the breach. • Identify possible risks faced by individuals and the company affected by a breach, and implementing programs to prevent similar issues from recurring. • Coordinate the investigation of breaches and pursuing the progress of additional reporting and remedial actions. • Meet regularly with the relevant parties to discuss/resolve data privacy incidents/ issues. • Provide primary support in the event of an enquiry, inspection or investigation by the regulatory body including audits conducted by the NPC, internal and external auditor. • Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security.

Responsible Party (*Check applicability*)	Key Obligations
	• Advise DMCIHI and/or its PC's regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data). • Perform other duties and tasks that may be assigned by the BOD/President that will further the interest of data privacy and security and uphold the rights of the data subjects.
Privacy Coordinators(PC's)	• Support the DPO in the implementation and enforcement of controls arising out of the Data Privacy Policy. • Maintain a Company-wide view of business processes impacting privacy, and the nature, size and sensitivity of personal information held by the Company. • Coordinate efforts for periodic privacy compliance reviews. • Assist the DPO in conducting PIAs at the initiation of any new/ modified business process, facility, service or technology that may impact the Company's privacy posture. • Ensure that privacy risk mitigation strategies are implemented, under the guidance of the DPO. • Respond to data breach notifications as per the defined data breach response plan. • Ensure that registrations and notifications are maintained and are up to date. • Periodically meet with and report to DPO for updates and realignment on data privacy concerns.
Administrative and Human Resources Department	• In coordination with the DPO, establish and implement relevant security controls standards in relation to physical records of the company. • Purge data in accordance with the established data retention policy. • Ensure on-boarding employee orientation includes data privacy. • Arrange and/or provide regular training/refresher for employees, in coordination with DPO as required for effective implementation

Responsible Party (*Check applicability*)	Key Obligations
	of the Data Privacy Policy. Keep track and maintain attendance records of DPA training sessions. • Ensure that appropriate disciplinary action is taken in the event of breaches. • In coordination with DPO, conduct PIAs on all third parties that may process personal information controlled by DMCIHI. • Arrange and/or provide DPA training for Third Parties, as applicable, as required for effective implementation of the Data Privacy Policy. Keep track and maintain attendance records of DPA training sessions. • Ensure that contracts with Third Parties include Data Sharing Agreements, if personal information will be involved.
Legal & Permits Department	• Oversee development and monitor implementation of the Data Privacy Policy. Review any conflict between the policy/guidelines and any local law and make recommendations to DPO. • Provide legal advice for the implementation and management of Data Privacy Policy. • Ensure that all PIPs/service provider contracts are compliant with the DPA and its IRR. • Review and recommend for DPO's approval Data Sharing Agreements with affiliates/ third parties. • Review and recommend for DPO's approval Data Privacy Disclosure Statements applicable to DMCIHI. • Escalate material breaches to DPO, relevant authorities, and senior management, as appropriate.
Information Technology Department (ITD)	• In coordination with the DPO, set relevant IT security standards in relation to data privacy controls. • Institute a process for regular testing, assessing and evaluating the effectiveness of technical security measures. • Perform annual inventory review of data processing systems and ensure reconciliation with the inventory of data processing systems.

Responsible Party (*Check applicability*)	Key Obligations
Finance Department - Compliance	• In coordination with the DPO, help facilitate periodic privacy compliance reviews in relation to data privacy controls, either through the Internal Audit function or an independent Third Party auditor. • Ensure that data privacy controls are captured in the documented business processes of various business process units. • Perform annual personal information inventory review and ensure reconciliation with the information asset inventory. • Formulate mitigation strategies for identified risks to privacy arising from the Company's business operations, data collection practices, supporting technology, facilities and services exchanged with external parties.
Employees	• Understand their data privacy obligations and responsibilities based on the nature of their work and position and comply with the requirements of the Data Privacy Policy. • Immediately report any suspected data privacy security breach to the DPO/COP. • Immediately report lost laptop/lost Company information assets to the DPO/COP.

Appendix 2 Suggested Wording under the General Terms and Conditions for a DMCIHI Contract

"You agree to comply with the Data Privacy Act of 2012 (DPA) with respect to any personal data (as that term is defined in the DPA) which you may obtain in connection with the purposes stated in this agreement. In particular, you agree that you will not collect, use, store, and disclose any personal data except to the extent necessary for the purposes of this agreement. Further, you agree to implement appropriate security, technical and organizational measures as mandated in the Act, and to delete or return all personal data upon termination of this agreement, or at the instruction from DMCIHI DPO.

In the same manner, DMCIHI will comply with the DPA with respect to any personal data that it may obtain in connection with the purposes stated in this agreement. In particular, DMCIHI will not collect, use, store, and disclose any personal data except to the extent necessary for the purposes of this agreement. DMCIHI will implement appropriate security, technical and organizational measures as mandated in the Act, and to delete or return all personal data upon termination of this agreement, or at the instruction from your DPO. Further, you warrant that you have the authority to provide any personal data to us in connection with this agreement and that any personal data you may provide to us has been processed in accordance with applicable law."

Appendix 3 Guidelines in Conducting Privacy Impact Assessment

The Data Privacy Manual governs the transfers of personal data and sensitive personal data between the DMCIHI and its respective Personal Information Processor/s (PIP/s), as applicable. New systems and processes may require data to be processed, stored and accessed anywhere within the DMCIHI network or managed on behalf of DMCIHI by external service providers.

The following PIA has been created to understand and document the various data flows that may be created as a result of a new system or process and ensure all appropriate data privacy & confidentiality compliance obligations have been taken into account. The DMCIHI Data Privacy Team will work with the owners of the new system or process to ensure all data privacy & confidentiality action items are addressed and the system operates in a privacy & confidentiality compliant manner.

PIA should be completed when there are events that significantly change in the privacy environment. The significant events are as follows:

a. New or modification to the current process
b. New projects
c. Marketing initiatives
d. Changes in the IT System Infrastructure

A PIA can be used to demonstrate that the system owners and functional management have applied data privacy controls throughout the system development lifecycle. In addition, performing a PIA for proposed changes identifies any conflicts between the post-implementation state and the privacy framework. For example, the PIA prior to introducing a new business application will identify if the way personal information is shared by the new application is in violation of the Data Privacy Policy.

A PIA should be triggered by events that significantly change the privacy environment of DMCIHI or if an existing process which significantly affects the privacy rights of data subjects is identified. For example, the introduction of new technology may change the manner in which personal information is

stored and processed. In some cases, the technology may only collect personally identifiable information for a moment. For example, a security camera stream may capture the movements of an individual. While a record may not be maintained for later use, the initial capture and viewing may raise privacy concerns and a PIA could be required. Other instances of technology with privacy implications include: systems utilizing radio frequency identification devices (RFID), biometric scans, data mining, or location tracking.

In other cases, the technology may not be changing, but a program or system opts to use data from a new source such as a commercial aggregator of information. A PIA is required when such new sources of information are used.

The introduction of a new business process and notable changes to existing business processes may trigger a PIA for various reasons. New business processes may introduce new uses of personal information, new information systems and infrastructure supporting the changed processes, and new methods of collection, processing and disclosure. Some new business processes may require updates to agreements and contracts, potentially impacting the management of personal information.

For changes in the IT System Infrastructure, at minimum, the following triggers should be considered:

PIA Trigger	Description
Digitization of records	Converting paper-based records to electronic systems.
Anonymous to Non-Anonymous	Operations performed on existing personal information database changes anonymous information into Sensitive Personal Information (SPI) or personal information (PII).
Significant System Management Changes	New uses of existing IT systems, including application of new technologies, significantly changes how SPI or PII is managed in the system. For example, when the company employs new relational database

PIA Trigger	Description
	technologies or web-based processing to access multiple data stores, such additions could create a more open environment and avenues for exposure of data that previously did not exist.
Significant Merging	The company adopts or alters business processes so that databases holding PII are merged, centralized, matched with other databases or otherwise significantly manipulated. For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create privacy concerns not previously an issue.
New User Access Mechanism	User-authentication technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by users (including Third Party users).
External Sources	The company systematically incorporates into existing information systems, databases of personally identifiable information purchased or obtained from third parties or public sources. An exception to this trigger would be merely querying such a source on an ad hoc basis using existing technology.
New Uses	Business partners work together on initiatives involving significant new uses or exchanges of information in identifiable form, such as marketing for products and solutions developed as joint ventures. In such cases, the CLIENT Data Privacy Officer should be consulted and prepare the PIA.
Internal Flow or Collection	Alteration of a business process that results in significant new uses or disclosures of information, including incorporation into the system of additional PII.

PIA Trigger	Description
Alteration in Character of Data	New PII is added to a database or information collection and thus, raises the risks to personal privacy. For example, the addition of health or financial information may lead to additional privacy concerns that otherwise would not arise.
New Processes	Introduction of new business process that results in multiple triggers and changes to business agreements impacting management of personal information.

For a PIA performed on systems or projects prior to their implementation, responses to the PIA Questionnaire should be populated based on the planned system/ project specifications and processes.

For each of these systems/processes, the DMCI Holdings' Data Privacy team will work with the system/process owners to:

- Clarify what the system/process involves
- Review the Data Privacy Manual to establish what impact (if any) there is upon the system/process and conduct a PIA of current practices against legal and generally accepted privacy requirements
- Develop appropriate data privacy action items for the global system/process and ensure they are implemented. The action items may include such things as:
  - Data Privacy Fair Processing Notices for system users;
  - Suggested data retention standards for personal data processed in the system if none exist;
  - Detailed background analysis and guidance containing the information required by the DMCI Holdings' Data Privacy Teams; and
  - High level guidelines for system users.

  Refer to the DMCIHI Privacy Impact Assessment Questionnaire template.

NO MORE STATEMENT HEREAFTER

REVIEWING DEPARTMENTS

Department / Division	Name of Signatory	Signature	Date