GLOBAL PRIVACY POLICY

Article 1: Background & Purpose of Global Privacy Policy

1.1 Purpose

This Policy specifies the special rules applicable to the management of **"Personal Information"**, in addition to the rules w.r.t. Confidential Personal Information contained in the "Global Confidentiality Policy" and the rules w.r.t. business information in the Media Policy of the Company.

- In most cases, Personal Information is **"Secrecy A"** information (i.e. to be disclosed only to Associates of the respective Department handling such information) for purposes of the Global Confidentiality Policy.

This Policy applies whether such Personal Information is managed by Honda Cars India Limited (HCIL) or a third party.

1.2 Definitions

1. "Personal Information"

   For purposes of this Policy, "Personal Information" means Confidential Information which is the personally identifiable information of customers, associates (employees), or business partners, as defined by applicable laws, regulations, and industry standards.

2. "Personal Data"

   For the purpose of this Policy "personal data" means any data which relates to a natural person if that person can, whether directly or indirectly in conjunction with any other data, be identified from it and includes sensitive personal data.

3. "Protected Systems"

   For the purposes of this Policy, "Protected Systems" means those computers, computer systems or computer network to which the Indian Government, by issuing gazette information in the official gazette, has declared as a protected system.

4. “Collection”

   For the purpose of this policy “Collection“ means, in relation to personal data, any action or activity that results in the company obtaining, or coming into the knowledge or possession of, any personal data of another person.

5. “Communication”

   For the purpose of this Policy ”Communication” means a word or words, spoken, written or indicated, in any form, manner or language, encrypted or unencrypted, meaningful or otherwise, and includes visual representations of words, ideas, symbols and images, whether transmitted or not transmitted and, if transmitted, irrespective of the medium of transmission.

6. “Disclosure”

   For the purpose of this Policy “Disclosure” (with its grammatical variations and cognate expressions) means, in relation to personal data, any action or activity that results in a person coming into the knowledge or possession of any personal data of another person.

7. “Biometric Data”

   For the purpose of this Policy “biometric data” means any data relating to the physical, physiological or behavioral characteristics of a person which allow their unique identification including, but not restricted to, facial images, finger prints, hand prints, foot prints, iris recognition, hand writing, typing dynamics, gait analysis and speech recognition.

8. “Primary Purpose of Collection of Information”

   For the purposes of this Policy, “Primary Purpose of Collection of information” means to collect any information which is necessarily required by HCIL to perform one or more of its functions or activities which is collected by lawful and fair means and not in an unreasonable intrusive way.

9. “Secondary Purpose of Collection of Information”

   For the purposes of this Policy, “Secondary Purpose of Collection of information” means any purpose other than the “Primary Purpose of Collection of information as specified in Section 5.3.4 below.

1.3 Positioning of Policy

This Policy is intended to set minimum standard controls with respect to the handling of Personal Information in accordance with the local laws and regulations.

1.4 Amendments to Global Privacy Policy

1. Any revisions to this Policy shall be determined and approved by the Global Confidentiality Committee of HCIL.

2. This Policy shall be reviewed on an as-needed basis, but in any event at least every year, in order to continuously improve and enhance Honda's management of personal information and to meet changes in Honda's business environment or in the Indian legal environment(s) in which HCIL operates.

Article 2: Personal Information Management Organization

2.1 Chief Privacy Officer

1. As deemed appropriate by the Company Confidentiality Committee (for instance, where a strong centralized response to issues involving Personal Information handling is necessary), the Chairperson of Company Confidentiality Committee or his assignee shall be appointed as the "**Chief Privacy Officer"** of the Company.
   The Global Confidentiality Committee of HCIL has appointed Mr. Praveen Paranjape as the "Chief Privacy Officer". The Organization Structure of GPP is as per attached Annexure-1.

2. The role of Company's Chief Privacy Officer are specified as follows:

   (a) To proactively implement policies and programs to enhance the protection of Personal Information, to promote such programs, and to create training programs designed to bolster the handling of Personal Information;

   (b) To report to the Regional Confidentiality Committees and all other appropriate parties when a leakage or violation occurs within the Company, and to formulate and implement corrective measures; and

   (c) Wherever required, to act as the representative of the Company in collaborating with the government to formulate industry standards, regulations, and laws, and in responding to government requests.

(d) Such other responsibilities as may be required by law.

2.2 Role of Company Confidentiality Committee

The Company Confidentiality Committee shall assist the Chief Privacy Officer in performing the requirements of his office as listed in Section 2.1 (2) above.

2.3 Role of Regional Confidentiality Committee

The Regional Confidentiality Committees shall coordinate activities related to Personal Information on a regional level, as appropriate.

Article 3: Duties of Personal Information Manager

3.1 Responsibilities of Managers

1. For each system (of whatever kind) containing Personal Information collected or used by his or her Department, the Departmental Manager / HOD shall appoint a person to supervise the system and to ensure that appropriate confidentiality measures are in place. The Supervisor shall ensure that associates who handle Personal Information in the Department are identified and listed.

2. The Departmental Manager / HOD that collects or uses Personal Information shall bear responsibility for the proper maintenance and use of systems containing Personal Information within the Department.

3.2 Training

1. The Company Confidentiality Committee shall arrange to train associates regarding the appropriate handling of Personal Information and shall maintain a record of such training.

2. Where the handling of Personal Information is entrusted to a business partner, the Division/Departmental Manager, (HOD) of the Division/Department that collects or uses such Personal Information shall ensure that the business partner trains its associates regarding the handling of Personal Information. In addition, when the Division/Department Manager entrusts it to the business partner, the Division Manager must stipulate in a Contract that the business partner holds the training.

3.3 Assessment and List of Locations Where Personal Information is Stored

1. In order to evaluate the type of Personal Information collected or used by each Department, each Departmental Manager/HOD shall prepare a list of places

(including electronic systems) where Personal Information so collected or processed is stored and shall submit this list to the Confidentiality Committee.

2. Notwithstanding the preceding provisions, it is not necessary to list categories or types of Personal Information which have been classified as "**Secrecy B**" (i.e. information which is meant for use of the whole Company).

3. The Departmental Manager shall update the list required by this section when the Department stops collecting or using a listed type or category or information.

3.4 Supervision of Associates

Where a Division or Department collects, uses, or manages Personal Information, the Division or Department Manager shall ensure that associates under his or her supervision are appropriately trained with respect to the handling of Personal Information and that they understand the importance of handling such information with enhanced care, the systems for handling such information, and the consequences of failing to properly manage such information.

3.5 Outsourcing Management of Personal Information to Business Partners

Where it is necessary to outsource the collection or use of Personal Information to a business partner, the Divisional Manager/HOD shall:

1. Confirm that the business partner has sufficient systems, policies, and practices in place to protect such Personal Information, to a standard conforming with the Company's requirements for handling of Personal Information;

2. Conclude a Confidentiality Agreement with the business partner which shall include specific provisions describing requirements for handling of Personal Information;

3. Prohibit subcontracting in general with respect to handling of Personal Information and require that the business partner obtain the prior written agreement/consent of the Company if subcontracting with respect to handling of Personal Information is unavoidable;

4. Receive back any Personal Information collected, used, or maintained by the business partner as a result of its work upon completion of the outsourced work.

5. Require the business partner to refrain from using any Personal Information collected, used, or maintained as a result of the outsourced work for any other purpose.

Article 4: Collection and Use of Personal Information

4.1 Collection

HCIL will not collect personal information unless the information is necessary for one or more of its functions or activities and the information will only be collected by lawful and fair means not in any un-reasonably intrusive way. When the Company collects Personal Information, it shall state the use and purpose to which it shall put such information. There are instances where HCIL requests personally identifiable information to provide the web site visitor a service or correspondence (new vehicle information alerts, promotions and mailed brochures). This information, such as name, mailing address, e-mail address, type of request and possibly additional information, is collected and stored by HCIL in a manner appropriate to the nature of the data and is used to fulfill your request. Such information is used to improve the services provided by HCIL. It is never provided to any other company for that company's independent use. HCIL will never sell your personal information to any other company. HCIL also shares user information from time to time with affiliates and business partners such as its authorized Dealer body in order to provide consistent service, support and marketing to its existing and prospective customers.

4.2 Notification

At the time that HCIL collects Personal Information, HCIL shall notify the person to whom the Personal Information belongs. Such notification may take any form (as specified by the Company Confidentiality Committee) and shall include the following elements:

1. The identity of the HCIL contact information for the Company to whom the Personal Information belongs;

2. The manner in which Personal Information has been (or will be) collected (for example, the use of cookies in a web browser) and the purpose for which it will be used;

3. The estimated period for which the HCIL will maintain the Personal Information;

4. If necessary under local laws and regulations, the right of the person to whom the Personal Information belongs to request that HCIL correct, deletes, or suspend the use of the Personal Information, and the method of exercising that right;

5. Any other entities which may receive the information; and

6. Any other notice requirements provided by applicable local laws or regulations.

4.3 Consent

1. If required by applicable laws, regulations, or industry standards the Company shall obtain the agreement of the person to whom the Personal Information belongs with respect to the purpose of its use. Where such an agreement is not required by applicable laws, regulations, or industry standards, the Company shall give notice to the person to whom the Personal Information belongs.

2. Notwithstanding Paragraph 1 of this section, the Company need not obtain agreement or give notice to the person to whom Personal Information belongs under the following circumstances:

   (a) If the collection or use of the person's Personal Information is necessary for the completion of a contract or business arrangement with that person, and the person has agreed in advance to such collection or use;

   (b) If it is necessary to collect or use the Personal Information due to legal requirements.

4.4 Processing of Personal Data/information

By visiting the website of HCIL and by providing personally identifiable, the person providing such information understands and consents to the collection, use, processing, transfer and disclosure of your personally identifiable information in accordance with this Privacy Policy. Such consent shall be deemed to include

consent to transfer of the personally identifiable information to locations that may have different levels of privacy protection than in India.

4.5 Sensitive Personal Information of Persons who are Not Associates/Employees or Business Partners

1. In general, HCIL shall not collect or use the following types of information with respect to persons who are not Associates/Employees or business partners:

   (a) Passwords;

   (b) Financial Information such as Banks Accounts, credit cards, debit cards and other payment instrument details;

   (c) Sexual Orientation;

   (d) Biometric information;

   (e) Matters concerning the faith or religious beliefs of a person;

   (f) Race, ethnicity, family status, physical or mental disorders, and criminal history, except to the extent required or permitted by law;

   (g) Matters concerning execution of the right to organize, collectively bargain and any other group movement by workers;

   (h) Matters concerning political participation or beliefs of a person; and

   (i) The matters concerning health and medical treatment, and sex life.

4.5 Transfer of Personal Information between Countries

1. If required by applicable laws, regulations, or industry standards, HCIL collects or uses Personal Information and intends to transfer it across international boundaries; it will obtain the agreement of the person who owns the information.

2. If required by applicable laws, regulations, and industry standards, prior to transferring information collected by HCIL in foreign countries, HCIL shall notify the person to whom the Personal Information belongs before such transfer.

Article 5: Requests by Owners of Personal Information

5.1 Requests for Disclosure of Personal Information

1. With respect to Personal Information collected or used by HCIL, HCIL shall be prepared, if required by local laws and regulations and upon request by the person to whom the Personal Information belongs, to disclose the following:

    (a) The kind of Personal Information collected or used and, to the extent possible, the sources of such Personal Information;

    (b) The identity of any third parties, if any**,** to whom the Personal Information has been disclosed, and the reason(s) for such disclosure;

    (c) If the person has a right to request correction, deletion, or suspension under local laws or regulations, the disclosure shall so state; and

    (d) Any other information required by law.

2. The appropriate form of disclosure requests and of the disclosures themselves, including the security requirements necessary to verify the identity of a person requesting disclosure, shall be decided by the Confidentiality Committee of each Company.

3. The Department Manager shall have ultimate responsibility for determining whether a disclosure request for Personal Information has been appropriately made.

4. In addition, if the disclosure meets any of the following criteria, the Company Confidentiality Committee shall determine whether disclosure is appropriate:

    (a) If disclosure may threaten the life, body, property, or other right or interest of the person to whom the Personal Information belongs or a third party; and

    (b) If disclosure would violate applicable laws or regulations.

5. If a disclosure request was not appropriately made or the Company Confidentiality Committee determines that disclosure is inappropriate for the reasons listed in the preceding Paragraph, the Company shall timely notify the person to whom the Personal Information belongs of the denial and the reason for it.

5.2 Correction

1. HCIL will take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either:
   (a) is satisfied that it needs to be corrected; or
   (b) an individual requests that their personal information be corrected.

2. If required by local laws or regulations, HCIL shall create a procedure for the person to whom the Personal Information belongs to request that Honda correct the Personal Information.

3. The appropriate form for such requests will be determined by the Company Confidentiality Committee.

5.3 Deletion or Suspension of Use

1. If required by applicable laws or regulations, HCIL shall implement a method for the person to whom the Personal Information belongs to request deletion or suspension of use of the Personal Information when the following criteria are met:

   (a) If the Personal Information is no longer necessary for the purpose for which it was collected or used;

   (b) If the agreement to process the data is canceled, the valid period of agreement to keep the data has expired and there is not any legal ground to process the data; and

   (c) If the person to whom the Personal Information belongs objects to its further collection or use on legal grounds.

2. HCIL may elect to retain or continue the use of Personal Information that has been requested for deletion or suspension, if retention or continued use would:

   (a) Be necessary to protect the public good, whether for health and safety or other reasons;

   (b) Serve the purpose of historical, statistical, or scientific research; or

   (c) Be necessary to maintain compliance with applicable statutes or regulations.

3. The use of Personal Information shall be restricted in the following situations:

(a) While the Personal Information is being corrected, if the person to whom the Personal Information belongs has made a valid request for correction;

(b) When HCIL does not need the Personal Information for business purposes but it is being preserved as evidence; or

(c) If the person to whom the information belongs objects to deletion of Personal Information because the method of processing is illegal and the person to whom the information belongs requests HCIL to restrict its use until the validity of the processing method is established.

4. HCIL will not use or disclose personal information for a purpose other than the primary purpose of collection, unless :

(a) the secondary purpose is related to the primary purpose, and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;

(b) the individual has consented to the use or disclosure;

(c) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety; or a serious threat to public health or safety;

(d) the organisation uses or discloses the personal information in investigating a suspicion of unlawful activity or in reporting its concerns to relevant persons or authorities; or

(e) the use or disclosure is required or authorised by or under law.

5.4 Designation of contact for requests related to Personal Information

HCIL Confidentiality Committee shall establish a contact for inquiries related to personal information, including requests for deletion, correction, or suspension of use and prominently display that contact information to the public.

5.5 Grievance Officer

1. HCIL shall designate a Grievance Officer to address the grievances of its information providers including those of customers, associates (employees), or business partners. The Confidentiality Committee of HCIL has appointed Ms. Jyoti Singh, Manager – HR, as the "Grievance Officer".

2. HCIL shall publish the name and contact details of such Grievance Officer on their website.

3. The grievances so raised before the Grievance Officer appointed by HCIL shall be redressed within a month of the filing of such grievance.

Article 6: Action in case of Information Leakages that Include Personal Information

6.1 Reasonable Security Practices & Procedures to be Followed

1. HCIL shall have and implement reasonable security practices and standards for sensitive personal data information and information.

2. HCIL shall provide for adequate compensation as decided by the Regional Confidentiality Committee with the assistance of the Company's Chief Privacy Officer as well as the Grievance Officer.

3. HCIL shall take reasonable technical and organizational precautions to prevent the loss, misuse or alteration of any personal data/information stored with them.

4. HCIL shall store all the personal information provided to them on a secure (password and firewall protection) servers.

5. All electronic and financial transactions entered through the website of HCIL will be protected by encryption technology.

6. The information providers shall acknowledge that the transaction of information over the internet is inherently insecure and HCIL cannot guarantee the security of data sent to them over the internet.

6.2 Response to a Leakage Involving Personal Information

In the event of a leakage or loss of Personal Information, in addition to following the processes described in GCP Section 3.7 and 3.8, the Chief Privacy Officer of the Company (or the Company Confidentiality Committee, as appropriate) shall evaluate the scope of the leakage or loss, the identity of persons affected by the leakage or loss, the appropriate notice(s) to be given, and shall effect such notice(s).

In addition, the Chief Privacy Officer (or Company Confidentiality Committee, as appropriate) shall report any such incident to the Risk Management Officer and the Compliance Officer.

6.3 Dispute Resolution

1. Any dispute, controversy or claim arising out of or relating to the privacy policy of HCIL, or any breach thereof shall be settled by arbitration administered by a sole arbitrator, appointed by HCIL.

2. Any award rendered by the appointed arbitrator may be entered in any Court within India having sufficient jurisdiction thereof.

6.4 Consequences of Breach of Personal Sensitive Date & Penalty

1. Any unauthorized access of the computer system (or any personally sensitive information therein) by any individual, associate (employee) or partner, Director including independent director shall be punishable as per the Indian law in force and may attract a heavy penalty up to Rupees One Crore as provided under section 43 of the Information Technology Act, 2000 ("IT Act 2000").

2. Any unauthorized downloading, extraction, copying of data or any unauthorized introduction of computer virus of contaminants shall also be covered under the penalty as mentioned in Section 6.4(1) above.

3. If any individual, associate (employee) or partner conducts any mode of hacking with the intention or knowledge of causing wrongful loss or damage to any person, the person who accessed such information shall be punishable under Section 66 of the IT Act 2000 and such person may be imposed with a penalty of imprisonment of three years or fine up to Rupees two lakh or both.

4. Any individual, associate (employee) or partner who wrongly causes any computer resource to be either destroyed, deleted, altered or diminishes its value, shall also be liable to be prosecuted under Section 65 of the IT Act 2000 and may be either imposed with a penalty of imprisonment or fine up to Rupees two Lakh.

5. Any unauthorized access or attempt to secure access of any protected computer system or network by the government shall also attract criminal proceedings which would be initiated by HCIL.

6. Any unauthorized access of data stored in a Protected System in contravention of Section 70 of the IT Act 2000 by any individual, associate (employee) or partner

shall make the person who accessed such data liable for punishment of imprisonment which may extent to ten (10) years and also shall be liable to a fine.

7. Any individual, associate (employee) or partner Director including independent director who knowingly and intentionally discloses personal sensitive data and information without consent of the person concerned and in breach of a lawful contract shall have committed breach of confidentiality and piracy under Section 72 of the IT Act 2000 and shall be made liable for punishment of imprisonment for a term extending to three years and fine extending to Rupees Five Lakhs.

8. Any individual, associate (employee) or partner, Director including independent director who has been entrusted with the personal sensitive data/information if dishonestly misappropriates such information or coverts it into his own property, or dishonestly uses or disposes off that personal sensitive data/information in violation of this Privacy Policy and the Indian Law in force shall have committed Criminal breach of trust and shall be liable to be prosecuted under Section 406 of the Indian Penal Code, 1860.

6.5 Choice of Sharing Information

Any person may choose to share Personally Identifiable Information with HCIL. However, any participation in using our websites and providing Personally Identifiable Information is completely voluntary. Anyone can choose to unsubscribe and opt-out to certain communications and access, or update and delete their contact information, by contacting us at the email address/number or address specified below.

6.6 Accessing and updating your information

1. HCIL shall give assess to personal information held by it on request by the individual to which the information pertains to except:

   (a) in the case of personal information other than health information — providing access would pose a serious and imminent threat to the life or health of any individual; or

   (b) in the case of health information — providing access would pose a serious threat to the life or health of any individual; or

   (c) providing access would have an unreasonable impact upon the privacy of other individuals; or

   (d) the request for access is frivolous or vexatious; or

(e) the information relates to existing or anticipated legal proceedings between the organization and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

(f) providing access would reveal the intentions of the organization in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorized by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders; by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of India.

2. Any person registering for an account on the website of HCIL, can access and update certain information we have relating to their online account by signing into

the account and going to the “My Account” section of the Site. The registered user may also update or delete their contact information by emailing us at jyotisingh1@hondacarindia.com.

6.7 Privacy Policy effective date and Revision days

Occasionally we may update the privacy policy in order to reflect any changes to the website or our privacy practices. If we make any updates to this statement, including any updates reflecting material changes to our Online Behavioral/Interest-Based Advertising practices, the new statement will be posted to the website ten (10) days prior to the changes taking effect.

The effective date of this privacy statement is 17th December, 2016.

6.8 LIABILITY DISCLAIMER

1. THE INFORMATION, SOFTWARE, PRODUCTS, AND SERVICES INCLUDED IN OR AVAILABLE THROUGH THIS WEBSITE MAY INCLUDE INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY MADE TO THIS WEBSITE AND TO THE INFORMATION THEREIN.

   HCIL MAKES NO REPRESENTATIONS ABOUT THE SUITABILITY, RELIABILITY, AVAILABILITY, TIMELINESS, LACK OF VIRUSES OR OTHER HARMFUL COMPONENTS AND ACCURACY OF THE INFORMATION, SOFTWARE, PRODUCTS, SERVICES AND RELATED GRAPHICS CONTAINED WITHIN THE WEBSITE FOR ANY PURPOSE. ALL SUCH INFORMATION, SOFTWARE, PRODUCTS, SERVICES AND RELATED GRAPHICS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. HCIL HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO THIS INFORMATION, SOFTWARE, PRODUCTS, SERVICES AND RELATED GRAPHICS, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, WORKMANLIKE EFFORT, TITLE AND NON-INFRINGEMENT.

   HCIL SHALL NOT BE RESPONSIBLE FOR UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR TRANSMISSIONS OR DATA, ANY MATERIAL OR DATA SENT OR RECEIVED OR NOT SENT OR RECEIVED, OR ANY TRANSACTIONS ENTERED INTO THROUGH HCIL’S WEBSITE. IN NO EVENT SHALL HCIL AND/OR ITS SUPPLIERS BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER

INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF USE, DATA OR PROFITS, ARISING OUT OF OR IN ANY WAY CONNECTED WITH THE USE OR PERFORMANCE OF THE THIS WEBSITE/SERVICES, WITH THE DELAY OR INABILITY TO USE THE WEBSITE/SERVICES, THE PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR FOR ANY INFORMATION, SOFTWARE, PRODUCTS, SERVICES AND RELATED GRAPHICS OBTAINED THROUGH THIS WEBSITE/SERVICES, OR OTHERWISE ARISING OUT OF THE USE OF THIS WEBSITE/SERVICES, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF HCIL OR ANY OF ITS SUPPLIERS HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. IF YOU ARE DISSATISFIED WITH ANY PORTION OF THIS WEBSITE/SERVICES, OR WITH ANY OF THESE TERMS OF USE, YOUR SOLE AND EXCLUSIVE REMEDY IS TO DISCONTINUE USING THE WEBSITE/SERVICES.HCIL MAKES NO WARRANTY THAT ANY SERVICE ON THIS WEBSITE WILL BE UNINTERRUPTED, TIMELY, SECURE OR ERROR-FREE.

2. HCIL reserves the right to disclose any personal information about you or your use of the HCIL Site/Services, including its contents, without your prior permission if HCIL has a good faith belief that such action is necessary to:

(a) conform to legal requirements or comply with legal process;

(b) protect and defend the rights or property of HCIL or its affiliated companies; or

(c) enforce the terms or use.

Nothing contained in this Policy is in derogation of HCIL's right to comply with governmental, court and law enforcement requests or requirements relating to your use of the HCIL Site/Services or information provided to or gathered by HCIL with respect to such use. If any part of this Policy is determined to be invalid or unenforceable pursuant to applicable law including, but not limited to, the warranty disclaimers and liability limitations set forth above, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the Policy shall continue in effect.