DATA PROTECTION POLICY

1. Application

This Data Protection Policy ("**Policy**") is applicable to all partners, employees and licensed technical representatives of Hawkes Bay Underwriting Limited (IA Licence No. FA2078).

This Policy applies to the protection of personal data by Hawkes Bay HK, including Hawkes Bay Underwriting Limited, either in the employment context or as part of the provision of any product or service by us, whether in respect of current, past and prospective partners, employees, technical representatives, policyholders, claimants and other individuals.

All our partners and employees and licensed technical representatives will receive this Policy and will be notified of any major updates, revisions or replacements of this Policy by us from time to time by notice in writing (whether published electronically or by other means). Each partner, employee and licensed technical representative should observe and is bound by this Policy.

A failure to comply with the requirements set forth in this Policy can result in disciplinary or remedial action as and when appropriate which may be termination of employment in serious cases.

The Company will ensure that its agents, subcontractors, consultants and service providers are made aware that they are expected to comply with the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) ("**PDPO**") and with this Policy (as applicable) and will implement adequate and appropriate security measures when processing or using Personal Data of the Company.

2. Definitions

(i) "We", "our", "us" or "the Company" for the purpose of this Policy means Hawkes Bay Underwriting Limited.

(ii) "Personal Data" will have the same meaning as defined in the PDPO (and any of its successor, replacement or amendment), namely any data (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable.

(iii) "Processing" in relation to Personal Data will have the same meaning as defined in the PDPO (and any of its successor, replacement or amendment), namely to include amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise.

(iv) "Using" in relation to Personal Data will have the same meaning as defined in the PDPO (and any of its successor, replacement or amendment), namely to include disclose or transfer the data.

3. Overview of the Company's Policy

We treat protection of privacy in relation to Personal Data very seriously. We are committed to safeguarding and managing Personal Data in compliance with the PDPO, including but not limited to the following six data protection principles under Schedule 1 to the PDPO ("**DPPs**") :-

(i) DPP 1 : purpose and manner of collection of personal data
(ii) DPP 2 : accuracy and duration of retention of personal data
(iii) DPP 3 : use of personal data
(iv) DPP 4 : security of personal data
(v) DPP 5 : information to be generally available
(vi) DPP 6 : access to personal data

Apart from the PDPO, the Company should also comply with the relevant guidance notes issued by the Office of the Privacy Commissioner for Personal Data, Hong Kong ("**PCPD**"), in particular but not limited to the Guidance on the Proper Handling of Customers' Personal Data for the Insurance Industry and the applicable requirements of the Hong Kong Insurance Authority ("**IA**").

This Policy is to be read conjunction with our Company's "*Document Creation, and Retention and Disposal Policy*".

All our partners and employees and licensed technical representatives should at all times respect the confidentiality of and keep safe any and all Personal Data collected, held, processed, stored or used for, or on behalf of, the Company.

4. Collection of Personal Data

The Company will collect necessary and adequate, but not excessive, personal data by lawful and fair means for lawful purposes directly related to our functions, activities and services.

A non-exhaustive indicative list of Personal Data that may be collected in connection with the Company's functions, activities and services is set out in Annex 1.

All practicable steps should be taken to notify the individuals of:-

(i) the purpose of data collection and the purpose of which the data are to be used;
(ii) the classes of persons to whom their Personal Data may be transferred;

(iii) whether such collection is obligatory or voluntary;
(iv) the consequences arising if the individual fails to supply the data; and
(v) the right to access and make correction of the data.

5. Accuracy of Personal Data

The Company will take all reasonably practicable steps to ensure that all Personal Data collected or retained are accurate, having regard to the purposes for which they are to be used.

Personal Data should not be used where there are reasonable grounds for believing that they are inaccurate, having regard to the purposes for which they are to be used.

The Company fully complies with the relevant obligations concerning an individual's rights of access and correction of Personal Data under the PDPO. In particular, where an individual legitimately requests access to and/or correction of his/her Personal Data, we should provide and/or correct such data in accordance with the manner stipulated in the PDPO. For details of the Company's policy on access and correction of Personal Data, please see section 10 below.

Where applicable, we should verify Personal Data including obtaining copies of certain identity documents such as proof of address and personal identification document. For the purpose of ensuring accuracy or authenticity of the identity document supplied to us, we may further validate such data against the pre-existing data held by the Company.

6. Retention of Personal Data

All practicable steps must be taken to ensure that Personal Data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used.

Personal Data which are no longer necessary for the fulfilment of the purposes (including any directly related purpose) for which they are to be used should be erased (by secure means) unless :-

(i) any such erasure is prohibited by law; or
(ii) it is in the public interest (including historical interest) for the data not to be erased.

In doing so, the Company will not retain Personal Data longer than is necessary for the fulfilment of the purposes for which it is collected, unless the Personal Data is also retained to satisfy any applicable legal or regulatory requirements, for example those as set out in Annex 2.

We should ensure all Personal Data retained is protected by the same security measures as set out in section 8 below.

7. Use of Personal Data

The Company will use Personal Data only for purposes for which the data were to be used at the time of the collection of the data, unless voluntary and express consent for a change of use is obtained from the relevant individual, or such use is required or permitted by the PDPO.

All Personal Data held by the Company will be kept confidential but we may, where necessary to satisfy the relevant purposes or directly related purpose, transfer or disclose such information to authorized third parties or as required or permitted by the PDPO.

The Company may transfer or otherwise process Personal Data collected from an individual in a jurisdiction outside of that jurisdiction. All such cross-border flows shall be done in accordance with the PDPO and the data privacy laws of that jurisdiction.

8. Security of Personal Data

We treat the security of our Personal Data as one of the top priorities. We should ensure that Personal Data will be protected against unauthorized or accidental access, processing or erasure. In doing so, the Company has physical, electronic and managerial measures and controls in place to safeguard and secure Personal Data. The Company and each of its partners, employees and licensed technical representatives are responsible for the Personal Data they hold.

The Company's policy on the security of Personal Data is set out in Annex 3.

9. Information to be Generally Available

The Company will take all reasonably practicable steps to ensure that an individual is informed of the kinds of Personal Data we hold, the main purposes for which the data is to be used and the classes of persons to whom the Personal Data may be transferred.

An individual may also have the right to ascertain the Company's policies and practices in relation to Personal Data, including but not limited to this Policy.

10. Access and Correction of Personal Data

Under the PDPO, an individual may have the right to :-

(i) ascertain whether the Company holds any Personal Data relating to them and, if so, obtain copies of such data; and

(ii) require the Company to correct Personal Data in its possession that is inaccurate for the purpose for which it is being used by means of a data access request.

An individual himself or herself, or a relevant person on his or her behalf, may exercise his or her right of access and correction. A relevant person refers to :-

(i) a person authorized in writing by the individual to make the request;
(ii) where the individual is under 18, his or her parent;
(iii) where the individual is incapable of managing his or her own affairs, a person appointed by a court to manage those affairs; or
(iv) where the individual is mentally incapacitated, his guardian appointed, or the Director of Social Welfare or any other person in whom his or her guardianship is vested or by whom the appointed guardian's functions are to be performed, under the Mental Health Ordinance (Cap. 136).

The primary contact person for any access and correction in relation to Personal Data is our Compliance Officer.

While no particular form is mandated, an individual should be encouraged to submit a data access request using the form of the prescribed "Personal Data (Privacy) Ordinance – Data Access Request Form" from the PCPD website, along with appropriate proof of identity (e.g. a copy of the individual's ID card) to the Compliance Officer. A reasonable fee may be charged for this service. There is no prescribed form for data correction request.

Upon satisfying itself of the authenticity and validity of the data access request and/or the explanation of the inaccuracy which is to be corrected, the Company should comply with such data access request or data correction request within 40 days after receipt of the same, unless the Company may under the PDPO limit or reject it.

11. Direct Marketing

The Company should not use any Personal Data for any direct marketing purpose or otherwise to provide any Personal Data to third parties for use by such third parties in direct marketing unless the individual's explicit consent has been received and has not been subsequently withdrawn.

When obtaining an individual's consent, the individual has to be notified how the Personal Data will be used for direct marketing.

When using an individual's Personal Data in direct marketing for the first time, the individual should be informed that he or she could request, without charge, for cessation to have his or her Personal Data used in direct marketing.

12. Training & Awareness

The Company provides regular training to ensure that all partners, employees and licensed technical representatives are aware of their obligations in respect of the security of Personal Data. Failure to complete any of the training courses may lead to disciplinary or other remedial action.

Advice should be sought from our Compliance Officer where necessary. The Compliance Officer is responsible for providing day-to-day assistance and guidance in relation to data protection matters.

All managers have a responsibility to ensure that effective controls exist within their areas of responsibility in line with this Policy. Senior Management will need to periodically confirm that their business areas follow this procedure.

13. Data Breach Reporting

A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use. It can include access or other deliberate action by an unauthorised third party, deliberate or accidental action (or inaction) by the Company and/or its service providers and/or data processors, sending personal data to an incorrect recipient, computing devices containing personal data being lost or stolen, alteration of personal data without permission, and loss of availability of personal data.

A data breach may cause threat to personal safety, identity theft, financial loss, humiliation or loss of dignity, damage to reputation or relationship, and loss of business and employment opportunities.

We have to take remedial measures to lessen the harm or damage that may be caused to the data subjects in a data breach and should at the same time consider the possible impact of the breach on the data subjects.

If a data breach is suspected to have occurred or is detected, it should be internally reported immediately to our Compliance Officer and IT Officer by email. Partners, employees and licensed technical representatives of the Company should never report a data breach to any external party (including but not limited to the affected data subjects). Our Compliance Officer is responsible for this and all external notifications need to be approved by him/her.

We should adopt the following action plan when a data breach is detected :-

(i) Immediate gathering of essential information relating to the breach;

(ii) Contacting the interested parties and adopting measures to contain the breach;

(iii) Assessing the risk of harm;

(iv) Considering the giving of data breach notification.

Details of the above action plan are set out in Annex 4.

Our Compliance Officer assumes the overall responsibility in handling data breach incidents, including leading the initial investigation and producing report of the findings of the investigation.

Annex 1

In relation to users of the Company's functions, activities and services

- Full name
- Nationality
- Mobile phone number
- Date of birth
- Photocopy of one or more identity documents
- Residential address
- Photocopy of address proof
- Occupation
- Bank account or credit card details
- Policy information, such as policy name and policy number
- Medical records
- Financial information
- Claims information

In relation to employees of the Company

- Full name
- Nationality
- Mobile phone number
- Date of birth
- Photocopy of one or more identity documents
- Residential address
- Photocopy of address proof
- Education and professional qualifications
- Employment history
- Salary and allowances
- Bank account details
- Job applications
- Appraisal reports
- Medical records

Annex 2

Policyholders and claimants

1. According to the Guidance on the Proper Handling of Customers' Personal Data for the Insurance Industry issued by the PCPD, in general, insurance institutions (which includes licensed insurance agencies) may retain personal data for not more than 7 years after the end of the business relationship, e.g. a customer withdrew his or her policy, for the purposes of complying with the various legal or regulatory requirements for keeping books of accounts or customer's records, the handling of potential litigation, etc. However, different types of personal data may warrant different periods of retention which may be shorter or longer than 7 years, and each case has to be considered on its own circumstances. In this regard, the Company may from time to time determine that there should be shorter or longer required time period for retaining specific types of business records due to legal or regulatory requirements or internal decisions.

2. The Company will retain the following documents or records relating to customer identity for anti-money laundering purposes:-

   (i) Any data and information obtained in the course of identifying and verifying the identity of the customer and/or beneficiary (if applicable); persons who purport to act on behalf of the customer
   (ii) Any additional information in respect of a customer and/or beneficiary that may be obtained throughout the customer due diligence and ongoing monitoring process, including simplified due diligence or enhanced due diligence;
   (iii) Where applicable, any data and information on the purpose and intended nature of the business relationship;
   (iv) Any records relating to the customer's account (e.g. account opening form, insurance application form or risk assessment form) and business correspondence with the customer (which at a minimum should include business correspondence material to customer due diligence measures or significant changes to the operation of the account); and
   (v) The results of any analysis undertaken (e.g. inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent or lawful purpose.

3. All of the above know your client / customer due diligence documents or records for anti-money laundering purposes will be kept throughout the business relationship with the customer and for a period of 5 years after the end of the business relationship / the relevant customer account is closed. For records which contain personal data (such as

names of bank account holders who are individuals), the data must not be kept longer than necessary.

Employees

4. Personal data of unsuccessful applicants may be retained for a period of up to 2 years from the date of rejecting applicants and should then be destroyed. The data may be retained for a longer period if there is a subsisting reason that obligates you to do so, or the applicants have given their consent for the data to be retained beyond 2 years.

5. Personal data of a former employee may be retained for a period of up to 7 years from the date of the former employee ceases to be employed. The data may be retained for a longer period if there is a subsisting reason that obligates the employer to do so, or the data is necessary for the employer to fulfil contractual or legal obligations.

Annex 3

1. *Access to Personal Data*

Access to records and information containing Personal Data without authorization is strictly prohibited. All partners, employees and licensed technical representatives are subject to a duty of confidentiality at all times regardless of location. Access to Personal Data is limited to those partners, employees and/or licensed technical representatives on a "need to know" basis that is commensurate with the individual's responsibilities.

2. *Physical Data*

(i) The Company has physical security controls including controlled access to premises, video surveillance, anti-intrusion alarm and smoke detectors to secure Personal Data against unauthorised and/or accidental access, processing, erasure, loss, disclosure, destruction and/or damage.

(ii) We operate a clear desk policy. Physical records containing Personal Data should be securely stored in locked cabinets when not in use.

(iii) All papers containing Personal Data should be shredded and destroyed after use.

(iv) Transfer of paper documents out of office premises should be avoided. If it is necessary, all Personal Data and restricted information on such documents should be redacted or removed before the documents are taken away from the office. Each partner, employee and licensed technical representative should maintain a register to keep track of the documents they have taken home and returned to office premises. There should be no disposal of paper documents with Personal Data outside of office premises.

3. *Electronic Data*

While no method of transmission over the Internet, or method of electronic storage can be guaranteed to be 100% secure, we will protect against any unauthorized access to the maximum extent reasonably possible.

Electronic Personal Data are stored in computer systems and storage media to which access is strictly controlled and/or are encrypted, located within restricted areas and/or protected by other appropriate measures to prevent unauthorized access or alteration.

All our partners and employees and licensed technical representatives will receive our Information Security Policy and will be notified of any major updates, revisions or replacements of the Information Security Policy by us from time to time by notice in writing (whether published electronically or by other means). Each partner, employee and licensed technical representative should observe and is bound by our Information Security Policy.

The following are some relevant measures and controls in place on information security of electronic Personal Data (for details please refer to the Information Security Policy) :-

(i) Requirement of complex passwords (with a combination of letters, numbers and/or symbols) to gain access to any system.

(ii) Regular backups for all electronic data and encryption of backups for offsite storage.

(iii) All electronic data can only be used on equipment or electronic devices issued or approved by us or via the secure corporate website operated by us. In particular, all electronic and portable devices (e.g. smartphones and notebook computers) should :-

- be encrypted with strong password which should be changed regularly;
- use multi-factor authentication (if available);
- perform regular system updates;
- install proper anti-virus and -malware software, firewalls and the latest security patches;
- have remote wipe function enabled so that information in the devices can be erased if they are lost;
- not be left unattended away from the office premises unless they are locked away in a secured place;
- avoid putting the names, logos and other identifiers of the Company on the devices conspicuously to avoid unwarranted attention.

(iv) Only corporate email accounts should be used for sending and receiving work-related documents and information, and documents containing Personal Data should be encrypted before sending out.

(v) Electronic devices provided by the Company should not be shared with any third party and personal devices (e.g. personal USB flash drive) should not be inserted into electronic devices provided by the Company.

(vi) All electronic devices and IT equipment provided by the Company must be returned upon termination of employment and/or service contract.

(vii) All computer systems have access control lists which ensure document usage can be controlled at an individual level as well as role or group level. All Personal Data usage is subject to audit.

(viii) When using video conferencing software, software with end-to-end encryption is preferred. A unique meeting ID with password should be set for each video conference. The meeting ID and password should be provided to intended participants only.

(ix) The security of VPN is ensured by, for example, using multi-factor authentication for connecting to the VPN, keeping security setting of the VPN platform up-to-date, using handshake protocol for establishing secure communication channels between electronic devices and our corporate networks, using full-tunnel VPN where possible, and blocking the connection from insecure devices.

(x) Network segmentation is implemented to reduce the risk and magnitude of data breach incidents and enhance the protection of critical and sensitive data.

(xi) Remote access control is granted to those partners, employees and/or licensed technical representatives on a "need to know" basis that is commensurate with the individual's role and responsibilities.

(xii) Remote access accounts will be locked out after multiple failed login attempts.

(xiii) Logs of remote access will be reviewed to identify any suspicious activities.

4. *Use of Processors*

The Company carries out appropriate due diligence on its data processors, including assessment of their security measures, and engages its processors via written agreements containing data protection provisions in accordance with the PDPO. Just as other agents, subcontractors, consultants and service providers, the Company's data processors are made aware that they are expected to comply with the PDPO and with this Policy (as applicable) and will implement adequate and appropriate security measures when processing or using Personal Data held by the Company.

5. *Patching Policy*

(i) The firmware of the Company's electronic devices should be updated and patched regularly and promptly, but the updates and patches should only be downloaded from trusted websites.

(ii) All electronic devices issued by us run Microsoft operating systems and the Microsoft Office Suite. These are configured to automatically download and apply patches and updates via Microsoft Update services as soon as they are released.

(iii) CITRIX (our underwriting platform) is hosted by the vendor Reinfo Asia Limited and they will patch and update the platform in accordance with the terms of their contract. The Company will ensure that the relevant contract contains data security provisions in accordance with the PDPO.

(iv) Anti-virus and -malware detection programmes are configured to check for updates once every 2 hours.

(v) The above automatic updates and patches should not be disabled without our prior express consent.

Annex 4

Data Breach Action Plan

1. Immediate gathering of essential information relating to the breach

The following relevant information should be promptly gathered for assessing the impact on data subjects :-

(i) When did the breach occur?

(ii) Where did the breach take place?

(iii) How was the breach detected and by whom?

(iv) What was the cause of the breach?

(v) What kind and extent of personal data was involved?

(vi) How many data subjects were affected?

2. Contacting the interested parties and adopting measures to contain the breach

Having detected the breach, the Company should take steps to identify the cause of and stop the breach. Our Compliance Officer will inform the Human Resources Officer and/or senior management as and when appropriate, and will decide whether it is necessary to contact the law enforcement agencies (e.g. the police), the relevant regulators (e.g. the PCPD), the Internet company (e.g. Google) and/or IT experts for reporting, advice and assistance.

We will also adopt the following containment measures if applicable :-

(i) Stopping the system if the data breach is caused by a system failure;

(ii) Changing the users' passwords and system configurations to control access and use;

(iii) Considering whether internal or outside technical assistance is needed to remedy the system loopholes and/or stop the hacking;

(iv) Ceasing or changing the access rights of individuals suspected to have committed or contributed to the data breach;

(v) Notifying the relevant law enforcement agencies if identity theft or other criminal activities have been or are likely to be committed;

(vi) Keeping the evidence of the data breach which may be useful to facilitate investigation and the taking of corrective actions;

(vii) In the event that the data breach was caused by the act or omission of the data processor, the data processor is required to report the data breach to the Company and/or other relevant parties, take immediate remedial measures and to notify the Company of the progress.

3. Assessing the risk of harm

Our Compliance Officer will carry out risk assessment to determine the extent of harm that may be suffered by the data subjects in the data breach, e.g. whether there is a real risk of harm.

4. Considering the giving of data breach notification

Where data subjects can be identified and our Compliance Officer reasonably foresees a real risk of harm in a data breach, we will, as soon as practicable after detecting the data breach, formally notify the affected data subjects and the relevant parties, including but not limited to the law enforcement agencies, the PCPD, any other relevant regulators, and such other parties who may be able to take remedial actions to protect the personal data privacy and the interest of the affected data subjects.

Depending on the circumstances of the case, a notification may include the following information :-

(i) A general description of what occurred;

(ii) The date and time of the breach, and its direction (if applicable);

(iii) The source of the breach;

(iv) A list of the types of personal data involved;

(v) An assessment of the risk of harm as a result of the breach;

(vi) A description of the measures already taken or to be taken to prevent further loss, unauthorised access to or leakage of the personal data;

(vii) The contact information of our Compliance Officer for the affected data subjects to obtain more information and assistance;

(viii) Information and advice on actions the data subjects can take to protect themselves from the adverse effects of the breach and against identity theft or fraud; and

(ix) Whether law enforcement agencies, the PCPD and such other parties have been notified.

The notification should be done in writing. When data subjects are not identifiable immediately or where public interest exists, we may do a public notification through the Company's website, if such method is not going to increase the risk of harm to the affected data subjects.

Document owner	Compliance Officer		**Document Ref**	COMP-HK-002
Version	**Date**	**Reviewer**	**Updated information**	**Next review**
V1.0	22/8/2022	Joseph Lo & Elsa Wong	Full review and update to incorporate HK regulatory requirements	August 2023