Standards on Processing of Personal Information

Macquarie Korea Asset Management Co., Limited (the Company) has a Standards on Processing of Personal Information (the Standards) as follows in an effort to protect the personal information and rights of the principal of information (Information Principal) and to smoothly address the grievance suffered by the Information Principal related to the personal information pursuant to Article 30 of the Personal Information Protection Act (PIPA) and Article 27-2 of the Act on Promotion of Information and Telecommunication Network Utilization and Information Protection, etc.

Article 1. Purpose of Processing Personal Information

The Company processes personal information for the purposes described in each of the following sections. The processed personal information will not be used for any other purposes than as set out below. Unless otherwise permitted by relevant law, the Company will notify and where required obtain prior consent from information principals in case of any changes to the following purposes of use:

1. Management of Officers and Employees (related to the collection of information of officers and employees)

   - Personnel Management: Recruitment; retirement; promotion; performance evaluation; remuneration; rewards & sanctions; relocation; secondment; transfer; etc.
   - Career Management: Issuance of certificates regarding employment including certificate of employment, certificate of career or certificate of retirement and verification of relevant facts
   - Wage Management: Base salary; profit share; other compensation; allowance; retirement pension; etc.
   - Employee Benefits: Group life and medical insurance; medical aid; vehicle support; corporate housing; provision of loan; vacation; etc.
   - Tax/Insurance: Subscription to legally required insurance policies including the major public insurances; payment and deduction of taxes including income tax
   - Compliance/Performance of Contract: Performance of employment contract; compliance with any and all internal and/or Macquarie Group policies; fair treatment and provision of opportunities among employees; confirmation and management of persons subject to veterans compensation; performance of legal and administrative obligations required of the Company including under industrial security and health laws, foreign worker laws, financial laws and related regulations

- Security/Contact: Protection of information processed by the Company; maintenance, improvement and monitoring of security system; prevention of unfair and illegal activities which may occur within the Company and collection of evidence; sharing of contact information and establishment of emergency contact network, etc.
- Marketing: Provision of contact information to customers or other third parties for marketing or business purposes
- Compliance with Foreign Laws: Overseas affiliates' compliance with foreign laws and cooperation with overseas regulators for their supervision

2. Transaction with Customers (related to the collection of information of officers and employees of corporate customers or individual customer)

- Determine whether to establish (financial) transaction, and establishment, maintenance, performance, and management of the (financial) transactional relationship, etc.
- Investigation of financial accident, settlement of dispute, handling of complaints, etc.

Article 2. Items of Personal Information to be processed

(1) The items of personal information to be processed and method of collection thereof in order for the Company to attain the purposes set forth in Article 1 are as follows:

1. In case of Officers and Employees

- Mandatory Information

  - Name, photo, date of birth, resident registration number, address, home telephone number, mobile phone number, email, gender, military service, place of birth, family members (including family relation, name, age, occupation, co-habitancy, resident registration numbers of family members), emergency contact, etc.
  - Educational background (college/university, location, major, year of entrance and year of graduation, graduation, GPA, etc.), work experience (employer, title, responsible area, service period), qualifications, history of awards / disciplinary actions, dates of employment, department, title, duties, etc.
  - Information on accounts with financial institutions used for wage transfer and/or trading of financial investment products

- E-mails received and sent via Company e-mail account, telephone conversation via office telephone and instant messenger communications via the Company's communication network
- Physical access records, logon records, work attitude, performance results, evaluation of customer relationship
- Video clips collected through CCTV

・ Optional Information
- Veterans compensation information, location of registration, vehicle license plate number, passport number

2. In case of Officers and Employees of Corporate or Individual Customers
Minimum personal information required to conduct business according to article 1.2.

(2) In principle, the Company does not collect sensitive information that may threaten to infringe upon the privacy of the Information Principal. If necessary, the Company collects sensitive information by obtaining additional consent of the Information Principal and uses the same only for the limited purposes so consented; provided, however, that the Company checks the accuracy and currency of the sensitive information on a regular basis.

(3) The information of employees is collected via webpage, interview, document, fax, telephone, e-mail, information collection program, etc, from time to time as needed. However, the information of individual customer or officers and employees of corporate customers, on the presumption that the providing corporate customer duly provides the personal information of relevant officers and employees, is collected via various documents including business card, transaction document or working group list, telephone, e-mail, etc.

Article 3. Period of Process and Retention of Personal Information

The personal (credit) information of the Information Principal collected for the purposes described in Article 1 will be retained and used until the above stated purposes of provision are all accomplished. The concerned personal (credit) information will be destroyed when it is confirmed to be unnecessary unless there exists an obligation to retain it pursuant to the laws and regulations.

Article 4. Provision of Personal Information to a Third Party

(1) In principle, the Company will process the Information Principal's personal information within the scope of the purpose outlined in Article 1 and will not process information exceeding the primary scope or provide it to a third party without the consent of the Information Principal in advance. However, in any of the following cases, except where there is a concern of unfairly infringing upon the interests of the Information Principal or a third party, the personal information may be used for other purposes or provided to a third party.

1. When the Information Principal has agreed on the provision and disclosure of information to a third party in advance.

2. When there are special provisions in other laws.

3. When the personal information is clearly acknowledged as necessary for the purpose of urgency in life, body or property profits as the Information Principal or his/her legal representatives are not in a condition to express his/her intention, or prior consent cannot be obtained due to address unknown, etc.

4. When personal information is provided in forms that make it impossible to recognize a specific individual, as is necessary for the purpose of statistics preparation and studies and researches, etc.

(2) The Company provides the staff's personal information as stated in each item below.

- Provided party: affiliates, partners, regulators, etc.

- Purpose of use of provided party: communication, employee/labor management, performance of employment agreement, compliance with laws and regulations, etc.

- Items of personal information provided: an individual's identifiable information, educational background, work experience, etc.

- Retention period of personal information: the personal information will be retained and used until the above stated purposes of provision are all accomplished. The concerned personal (credit) information will be destroyed when it is confirmed to be unnecessary unless there exists an obligation to retain it pursuant to the laws and regulations.

- Employees may refer to the Macquarie network for details.

(3) When the Company obtains consent of the Information Principal or provides personal information in accordance with Article 15, Paragraph (1), Items 2, 3 and 5 of the PIPA, the

Company will not notify the Information Principal of each of Article 17, Paragraph (2) of the PIPA and the Information Principal's right to request inspection, correction, deletion and suspension of processing of, the personal information.

Article 5. Delegation of Personal Information Processing Services

(1) In principle, the Company does not delegate the processing of the concerned personal information to others without the consent of the Information Principal. However, in each of the following cases as set forth in Article 26 of the PIPA, the Company may delegate the processing of personal information.

1. Service provider: accounting firms (or similar service providers), data storage center, etc.

2. Purpose of delegation: performance of delegated services, etc.

3. Items of personal (credit) information provided: individual's identifiable information, distinct identifiable information, salaries, etc.

4. Retention period of personal information: the personal (credit) information will be retained and used until the above stated purposes of delegation are all accomplished. The personal (credit) information will be destroyed when it is confirmed to be unnecessary unless there exists an obligation to retain it pursuant to the laws and regulations.

(2) When executing a service agreement, the Company clearly sets forth the compliance with personal information protection related laws, the prohibition of provision of personal information to a third party, and where the responsibility lies, and maintains the terms and conditions of the service agreement both in writing and in electronic form. The Company will notify any changes to the service providers by email and by amending and publishing this Privacy Policy.

Article 6. Rights and Obligation of Information Principal and Method of Exercise

(1) The Information Principal may request to inspect his/her own personal information or that of children under age 14 (applicable only to their legal representatives) that are processed by the Company.

(2) The Information Principal who inspected his/her own personal information may request the Company to correct or delete his/her personal information that are not verifiable or inconsistent with the facts. However, in cases where such personal information is stipulated to be collected in other laws and regulations, the Information Principal may not request the deletion of such information.

(3) In cases where the Information Principal requests correction or deletion of personal information, relevant personal information will not be used or provided until the correction or deletion is completed. In such cases, if incorrect personal information has been used or provided, such personal information will be immediately corrected.

(4) The Information Principal may request the Company to suspend the processing of his/her own personal information. However, in any of the following cases, the Company may refuse such request after notifying the Information Principal of the reason of such refusal:

1. If there is a special provision in laws or it is inevitable to refuse such request to comply with its obligations under applicable laws or regulations;

2. If such an act will likely to inflict damages upon another person's life or body or unfairly infringe upon another person's properties and other interests; or

3. If it is difficult to carry out any contract due to failure in providing services agreed with the Information Principal or otherwise, unless relevant personal information is processed, but the Information Principal has not expressly expressed his/her intention of termination of such contract.

(5) The personal information that is terminated or deleted by the Company upon request of the Information Principal will be disposed of pursuant to the period of process and retention of personal information under Article 3 hereof.

Article 7. Destruction of Personal Information

(1) If the expiration of the retention period of personal information, the Company will destroy such information as soon as practically possible from the expiration date of the retention period, unless any of the followings occurs. If such personal information becomes no longer needed for reasons that the purpose of processing such information has been achieved, the business has been closed, etc, the Company will destroy such information as soon as practically possible from the date on which the processing of such information is deemed unnecessary, unless any of the following occurs:

1. If any laws and regulations require the preservation of such personal information; or
2. If there are any other similar justifiable reasons.

(2) Any printout, document, etc. containing personal information will be destroyed by incinerating or shredding them into pieces, and personal information in the form of electronic file will be destroyed by permanently deleting it in an irrevocable manner.

Article 8. Measures to Ensure Safety of Personal Information

The Company takes following technical, administrative and physical actions required to ensure the safety of personal information in accordance with Article 29 of the PIPA:

1. To minimize the number of employees to handle personal information and provide training for them.
   The Company designates employees to handle personal information, and implements measures to minimize the number of employees to manage personal information.
2. To conduct a periodic self-audit.
   The Company conducts a regular audit in order to ensure the stability of handling of personal information.
3. To establish and implement internal management plan.
   The Company may establish and implement an internal management plan for the safe handling of personal information if necessary.
4. To encrypt personal information.
   Passwords, biometric information and, if deemed necessary, other related personal information of users' are stored and managed after encryption. Data files containing personal information are to be encrypted or locked before being sent electronically.
5. To take technical measures against hacking, etc.
   The Company installs and periodically updates and inspects security programs to prevent the leakage of and damage to personal information due to hacking or computer viruses, etc. Further, the Company installs security systems and technically/physically monitors and blocks the restricted area.
6. To control access to personal information.
   The Company takes necessary measures to control the access to personal information by granting, changing and cancelling the right to access the data base system in which personal information is processed, and also controls unauthorized access from the outside by using adequate IT security systems described in item 5 above.
7. To retain log-in records and prohibit forgery and alteration of log-in records.
   The Company retains and manages log-in records to key personal information processing systems for at least six months, and adopts security functions in order to prevent forgery, alteration or loss of log-in records.
8. To adopt locking system for document security.
   The Company keeps the documents, auxiliary storage medium, etc. containing personal information in a safe place with locking system.
9. To control access from unauthorized persons.
   The Company has secured physical locations to keep personal information, and establishes and operates the access control process for such locations. [This provision complies with the Standards of the Ministry of Public Administration and Security ("MOPAS").]

Article 9. Privacy Officer Appointment

In order to protect personal information and deal with complaints about personal information, the Company designates Compliance manager (phone number: 822 3705 4950) as Privacy Officer under Article 31(1) of the PIPA.

Article 10. Installation and Operation of Imagery Information Processor

The Company installs and operates imagery information processor as follows.

1. Grounds and Purposes for Installation of Imagery Information Processor

   Facility safety, crime prevention, collection of evidences, etc. for the Company

2. Number of processors installed, location of installation, scope of filming
   - Number of installed processor: 1
   - Location of installation: major facilities including lobby and corridors of the office building of the Company
   - Scope of filming: entire space of the major facilities

3. Responsible manager and department and persons having access to the imagery information
   - Responsible manager and department: Manager of Business Services Department
   - Persons having access to the imagery information: Designated person in Business Services Department Manager, Privacy Officer, and persons who are authorized by the Privacy Officer

4. Imagery information filming hours, retention period and place, and processing method

   - Filming hours: 24 hours
   - Retention period: 30 ~ 60 days from filming
   - Retention place and processing method: retained and processed in the data centre operated by Business Services Division

5. Method for inspection of imagery information
   - Method: request to the manager described in Item 3. above

6. Measures in response to the request of the Information Principal for inspection, etc. of imagery information

In order for the Information Principal to access imagery information, he/she shall file an application for access with the Company in a form of application for inspection/confirmation of existence of the personal imagery information. The Company allows access to the imagery information only when the Information Principal himself/herself is filmed, or when it is explicitly required for benefit in life, body, and asset

of the Information Principal.

7. Technical, managerial and physical measures for protection of imagery information

For protecting imagery information, the Company takes actions including maintaining an internal management plan, control of access and restriction of accessing authority, safe storing of the imagery information, application of transfer technology, storing of processing records and measures for preventing forgery or alteration, preparation of storage facility and installation of lock.

Article 11. Amendment to the Standards

The Standards will apply from the enforcement date set out below. Any addition, deletion and correction of the Standards made pursuant to applicable laws and regulations will be notified via email seven days prior to the enforcement date of such change.

Article 12. Remedy for Infringement of Right

If the Information Principal needs to file a report or receive counseling with respect to the infringement of personal information, the Information Principal may contact the following organizations:

1. Personal Information Dispute Mediation Committee
2. Privacy Invasion Report Center in the Korea Internet Security Agency
3. Korea Association for ICP Promotion
4. Hi-tech Crime Investigation Center of the Supreme Prosecutors' Office
5. Cyber Terror Defence Center of the National Police Agency

Addendum(24 August 2012)

The Standards shall take effect as of the date approved from MKAM board.

Addendum(24 June 2014)

The Standards shall take effect as of 24 June 2014.

Addendum(31 October 2016)

The Standards shall take effect as of 31 October 2016.