DEIB POLICY
(Diversity, Equity, Inclusion, and Belonging Policy)

I. INTRODUCTION

Throughout JTB's history, the company has prioritized equitable inclusion of people of all gender identities, ages, races, ethnicities, national origins, cultures, religious or political beliefs, languages, education levels, socioeconomic backgrounds, family or relationship statuses, sexual orientations, genetics, and/or abilities. JTB's corporate culture has always embraced diversity, respected diverse values and welcomed innovation.

In April 2011, JTB implemented the JTB Group Codes of Conduct ("**Code**") to ensure consistent levels of quality service and employee conduct worldwide. The Code requires all JTB employees to adhere to the basic rules of conduct set forth therein, -

Ⅱ. COMMITMENT TO DEIB (DIVERSITY, EQUITY, INCLUSION, and BELONGING)

JTB is dedicated to fostering, cultivating and preserving a culture of DEIB. JTB believes that its employees are high-performing individuals who reflect the diversity of the communities where all JTB employees work and live.

This DEIB Policy ("**Policy**"), sets out JTB's commitment to continued DEIB practices which includes recruiting and retaining employees from diverse backgrounds and experiences, creating awareness of diversity issues and benefits, and fostering a supportive environment where inclusivity is expected and prioritized.

This Policy formulates the common understanding of what JTB considers diversity and aims to raise awareness among its employees of their rights and responsibilities pertaining to the issue.

Ⅲ DEFINITIONS

“Diversity” is the collective mixture of differences and similarities that includes individual and organizational characteristics, values, beliefs, experiences, backgrounds, sexual orientations, gender identity, preferences, and behaviors.

"Equity" is about ensuring all individuals are treated fairly and respectfully and have equal access to opportunities and resources.

“Inclusion” is the achievement of a work environment in which all individuals are ensured “Equity” and can contribute fully to the organization’s success. Without inclusive practices, a diverse environment cannot be achieved.

“Belonging” refers to employees’ sense that they are welcomed, accepted, valued, and empowered for their diverse backgrounds and experiences. An inclusive work environment helps foster a sense of belonging.

Ⅳ COMMITMENT TO A DIVERSE WORK ENVIRONMENT

JTB’s goal is to provide a working environment where all employees are included and valued for their contributions and to reflect the diversity of our clients and the communities in which we work. Outside of the obvious moral imperative of equity, research shows that diversity in the workplace can boost the quality of decision-making and encourage people to be “more creative, more diligent, and harder-working.”[1] Accordingly, when the individuals who shape the values and activities of our organization come from a wide array of backgrounds, we believe that they are able to each bring their own unique perspectives that solves problems and enhances JTB in potentially more innovative ways.

JTB is committed to providing equal opportunity employment; creating, managing, and valuing diversity in our workforce; providing a safe work environment; and fostering a culture of belonging where all employees are included, treated with dignity and respect, promoted on their merits, and placed in positions to contribute to our future success. We are guided by the principles of honesty, integrity, trust, and respect as we work together to meet our company and client objectives.

We embrace a diverse workforce and recognize and respect the qualities of all our employees, including, but not limited to, gender identities, age, race, ethnicity, national origin, culture, religious or political beliefs, language, education, veteran status, socioeconomic background, family or relationship status, sexual orientation, medical condition, genetics, and/or disability. We also value diversity of perspective including differences in personality, life and work experience, skills, ways of thinking and working, and other characteristics that make our employees unique.

JTB's commitment to DEIB extends to all areas of our business including recruitment, job assignment, compensation and benefits, talent development, skills enhancement, promotions, employee retention, flexible work arrangements, forms of leave available to employees, policies and procedures, board appointments, and succession planning.

Ⅴ JTB'S APPROACH TO DEIB

JTB is committed to DEIB by increasing our focus on recruiting and retaining employees from diverse backgrounds, creating additional awareness of diversity issues and benefits, fostering a more supportive environment where inclusivity is expected and prioritized, and embedding accountability for diversity throughout the organization.

In an effort to hold ourselves accountable and to support these corporate initiatives, JTB is in the process of creating an internal DEIB committee that will look into any suspected violations of this policy and will run company-wide trainings.

All JTB Representatives are responsible to:

A. Maintain respectful communication and cooperation between all employees;
B. Treat others with dignity and respect at all times; and
C. Report details of any suspected violation of such behavior performed either within JTB or through JTB's contractors, suppliers or other business partners.

Ⅵ COMMUNICATION AND AWARENESS OF THIS POLICY

All JTB Representatives are expected to exhibit conduct that reflects inclusion during work, at work functions on or off the work site, and at all other company-sponsored and participative events. All JTB Representatives are also required to attend and complete annual DEIB awareness training to enhance their knowledge to fulfil this responsibility.

Ⅶ REVIEW OF POLICY IMPLEMENTATION

The proper implementation of this Policy and subsequent trainings will be reviewed annually, where applicable.

Revision History

Version	Detail	Date
1.0	Newly developed	2021/5/1
2.0	Updated in accordance with reestablishing JTB Group Policy	2023/4/1
3.0	Revised its title in accordance with DEIB promotion	2023/10/1

ANTI-COMPETITIVE BEHAVIOUR POLICY

1. COMMITMENT TO FAIR AND ETHICAL COMPETITION

JTB IS FIRMLY COMMITTED TO THE PRINCIPLE OF DOING BUSINESS IN A FAIR AND ETHICAL WAY AND NOT ENGAGING IN ANTI-COMPETITIVE PRACTICES WITH ITS CLIENTS/CUSTOMERS, SUPPLIERS, BUSINESS PARTNERS OR COMPETITORS.

Laws – commonly called “antitrust laws” or “competition laws” – apply to protect free and fair competition in **all** of the countries in which JTB does business and apply to **all** Employees.

Violation of these laws will result in (i) large civil and criminal fines against JTB from global authorities (Japanese companies in particular have, for example, been fined hundreds of millions of Euros by the European Commission alone) and (ii) significant private damages claims against JTB from clients/customers and suppliers and (ii) may also result in personal fines and imprisonment for the Employees involved. Furthermore, such actions can severely damage JTB’s reputation.

These laws are complex and apply globally, no matter the Employee’s location. Employees who are unsure of the appropriateness of their business practices should consult with company management (“**Management**”) for additional clarification.

JTB will take immediate and appropriate action to prevent and correct Employee behaviour that violates this Policy and those laws.

2. DEFINITION OF ANTI-COMPETITIVE BEHAVIOUR

Each country has different labels and definitions for what is anti-competitive behaviour. However, there are consistent types of prohibited behaviour, as follows.

A. Collusion/Cartel

Collusion/Cartel involves the behaviour of two or more competitors where they agree with each other how they will compete (or appear to compete).

This behaviour may also be labelled, amongst other things, *cartels*, *anticompetitive agreements*, *bid-rigging*, *market allocation*, *price/strategy signaling* or *illegal information exchange*.

It may be a formal agreement (whether written down or not) or an informal arrangement or simply an unspoken understanding and covers:

- Fixing or maintaining prices, volumes or terms of supply of products and services;

- Allocating of clients/customers, suppliers, business partners or markets;

- Manipulating of bidding or tender processes; and

- Exchanging sensitive commercial information which may allow JTB to predict a competitor's course of action and so adjust the business accordingly (even without any mutual agreement to do so).

B. Abusing market position

Abusing market position involves the behaviour of one party alone where they have sufficient market power to force unfair terms or actions without sufficient business justification.

This behaviour may also be labelled, amongst other things, *abuse of a dominant position*, *monopoly power*, *tying*, *predatory pricing*, *boycotts*, *improper exclusive dealing*.

It covers:

- Tying products or services together to force clients/customers to take those that they don't necessarily want to obtain those that they do want;

- Selling a product or service at such low cost in order to damage or eliminate competitors and later increase prices; and

- Refusing to do business with a party without sufficient business justification in order to damage or eliminate business partners.

C. Other practices

Different countries may also impose restrictions on some of the following behaviours which involve unfair terms or actions without sufficient business justification:

- Collective bargaining/boycotts: where parties come together to negotiate with a supplier or customer; and

- Resale Price Maintenance: where minimum resale prices are set for products or services.

3. RESPONSIBILITY OF ALL EMPLOYEES

All Employees shall conduct their business relations ethically and compete fairly and shall comply with applicable competition and antitrust laws. The following guidelines will help maintain these standards in the business relationships with competitors, suppliers, clients/customers as well as trade associations and independent third parties.

A. Dealing with competitors (horizontal relationships)

- Do not fix prices with competitors.
- Do not allocate nor divide clients/customers, suppliers, business partners, territories or lines of business.
- Do not communicate with competitors in a bidding or tender situation.
- Do not share commercially sensitive information with a competitor in any setting (formal, informal or social).

  This includes: current or future prices, costs or volumes; terms of service; terms of supply; details of tenders or bidding submissions; strategic plans; market share data; distribution practices.
- Do not signal future pricing or strategy indirectly (i.e. through third parties) to competitors.

B. Dealing with suppliers and clients/customers (vertical relationships)

- Do not force clients/customers to take products or services they do not want or need.

- Do not sell a product or service at such low cost to damage competitors with the intent of later increasing prices.

- When proposing to bundle/tie products and services together, consult with Management **in advance**.

- When proposing to grant exclusivity of products and services, consult with Management **in advance**.

- Do not refuse to deal with another party without consulting with Management **in advance**.

C. Dealing with trade associations and independent third parties

- Be very careful sharing any information with a trade or equivalent association or independent service provider (e.g. a bench-marker). This may be possible if information is aggregated or blended **but** Management shall be consulted **in advance**.

- Report plans to attend any trade or equivalent association meeting to direct manager and, before attending such meeting, review this Policy in full and review the meeting agenda for inappropriate items. Consult with Management if in doubt.

- If discussions at such meetings start to cover competitively sensitive subjects, object and, if discussion continues, leave the room and ask that the departure is recorded in the minutes record. Report immediately to Management.

- Review minutes and records of any such meetings to ensure accurate or otherwise maintain detailed notes of such meetings.

D. Maintain awareness

It is all Employees' duty to at all times understand and comply with the Code and this Policy and attend any training assigned.

Failure to comply may result in disciplinary action, up to and including termination of employment and in some jurisdictions Employees may be personally and criminally liable.

4. RESPONDING TO ANTI-COMPETITIVE BEHAVIOUR

A. Internal reporting of behaviour

Employees do not need to deal with issues of anti-competitive behaviour alone. JTB is committed to taking appropriate steps to prevent, correct and end unlawful behaviour. However, this cannot be done without everyone's assistance.

Employees who suspect or believe that anti-competitive behaviour is occurring or has occurred shall immediately report the matter to Management regardless of who is engaged in the behaviour. If an Employee suspects and says nothing, he/she could be held criminally responsible and/or lose his/her position of employment.

Employees shall not delay in making such reports. Receiving information at an early stage is crucial in:

- Conducting a prompt investigation to gather reliable and complete information of the alleged behaviour; and

- If necessary, alert or respond to governmental authorities. Applications for immunity or leniency, for example, are possible in most countries and could prevent or reduce fines and reputational damage **if submitted quickly**.

Employees who file reports based on their honest belief will not be subject to reprisal or damage to their career, reputation or employment, even if the investigation reveals that such report was wrong, or based on a misunderstanding.

B. Responding to external authority investigations

Governmental authorities may investigate alleged anti-competitive behaviour following a complaint from a client/customer, supplier, business partner or competitor.

Authorities may request information from Employees and JTB. When receiving a request **immediately** report this to Management (and they will alert the legal department and appoint external lawyers).

Authorities may conduct an unannounced inspection (a *dawn-raid*) at JTB offices or Employees' homes. If subject to such an unannounced inspection (a dawn-raid), Employees shall:

- **Immediately** alert Management (and they will alert the legal department and appoint external lawyers).
- Co-operate with the investigators in a reasonable way i.e. respond honestly and accurately to factual questions, but do ask for a lawyer to be present.
- Do not destroy documents or evidence.
- Keep a record of the information supplied (documentary and verbally).

JTB is committed to full compliance with laws and regulations and requires every Employee to be equally committed when dealing with governmental authorities.

Revision History

Version	Detail	Date
1.0	Newly established	2015/4/30
1.1	Updated in accordance with Japanese version 2018	2018/9/28
2.0	Updated in accordance with reestablishing JTB Group Policy	2023/4/1

ANTI-CORRUPTION POLICY

1. COMMITMENT TO ANTI-CORRUPTION AND ANTI-BRIBERY

JTB IS FIRMLY COMMITTED TO MAINTAINING THE HIGHEST STANDARDS OF ETHICS AND HAS A ZERO-TOLERANCE TOWARDS BRIBERY AND CORRUPTION. JTB PROHIBITS ALL FORMS OF BRIBERY AND CORRUPTION, AS WELL AS ANY BUSINESS CONDUCT THAT COULD CREATE THE APPEARANCE OF BRIBERY AND CORRUPTION. JTB'S COMMITMENT TO THIS CAUSE REQUIRES STRICT COMPLIANCE WITH ALL APPLICABLE LAWS, PROHIBITING IMPROPER PAYMENTS, GIFTS, OR INDUCEMENTS OF ANY KIND TO AND RECEIVED FROM ANY PERSON, INCLUDING OFFICIALS IN THE PRIVATE OR PUBLIC SECTOR, CLIENTS/CUSTOMERS, AND SUPPLIERS.

A. Impact of Violation

If JTB is found to have participated in any bribery or corruption, it could face significant penalties, including but not limited to heavy fines, suspension or cancellation of business licences, or a prohibition from participating in bidding exercises in the public sector. Engagement in bribery and corruption may result in personal fines and imprisonment for the Employees involved in many jurisdictions. Furthermore, there would also be critical damage to JTB's reputation.

B. Recent Worldwide Trend

In recent years, international enforcement activities in respect of anti-corruption laws have been on the uptrend. Among the pieces of legislation that have featured significantly in this worldwide trend are the Foreign Corrupt Practices Act of the U.S. ("**FCPA**") as well as the Bribery Act of the U.K. ("**UKBA**").

These laws have cross-border application and may apply globally, regardless of the Employee's location. For example, if certain requirements for cross-border application under the FCPA and/or the UKBA are met, JTB and the relevant Employees may be punished by the relevant authorities of the U.S. and/or U.K. for any bribe given by an Employee to the public officials of any country in Asia, even if

the misconduct took place outside of the U.S. or U.K. and the recipient of the bribe is not a public official of the U.S. or U.K. There is always a risk of the cross-border application of these laws because such provisions of cross-border application may and can be interpreted and implemented by the relevant authorities very broadly.

Furthermore, there is also a notable trend whereby major developing countries, in which bribery and corruption had previously been prevalent, are now making serious efforts with respect to anti-corruption. These efforts include the increase in local enforcement of anti-corruption laws against private companies, especially against multi-national corporations.

C. General Responsibility of Employees

Employees who are unsure of the appropriateness or legality of their business practices should consult with the management of each company ("**Management**") for additional clarification. Management shall report and consult with JTB Corp. ("**JTB HQ**") based on the applicable group reporting rules if they have any material concerns as to the legality or propriety of any business practices of the company.

2. DEFINITION AND GENERAL PROHIBITION OF BRIBERY

A. No Offer, Promise, Payment, Solicitation or Acceptance of Anything of Value May Be Made to or Received from Public Officials, Private Persons or Companies with Corrupt Intent

(a) Corrupt Intent

An individual has Corrupt Intent if he/she has the following intentions:

(i) Intention of gaining from the recipient or principal of the recipient any commercial, contractual, or regulatory advantage for JTB in any way which is unethical; and

(ii) Intention of gaining from the recipient or principal of the recipient any personal advantage, monetary or otherwise, for the individual or anyone connected with the individual.

(b) Anything of Value

Bribes are not always a matter of handing over cash. Non-cash advantages may also be bribes.

In this Policy, Anything of Value shall include cash and any other form of direct or indirect benefit. Gifts, entertainment, excessive promotional activities, personal favours, the hiring of relatives, the giving of a job to a family member, the granting of a scholarship to a family member and the covering or reimbursing of expenses can be the basis for the violation of the applicable anti-corruption laws and the terms of this Policy.

For the avoidance of doubt, any gifts, reimbursement or payment which may be permissible under Section 2.C. below are prohibited if they are given or made with Corrupt Intent described in Section 2.A.(a) above.

(c) Public Officials

Public Officials in this Policy shall include, in any jurisdiction, employees or officers of:

- governments (including regional and local departments, councils and agencies) (e.g. national ministries or regional or local departments of tourism, local councils which issue and deal with required licences, etc.);
- enterprises owned or controlled by a government (e.g. an airport management company, a state-owned hotel, etc.);
- state-owned utility companies;
- political parties and party officials;
- candidates for public office; and
- public international organisations (e.g. U.N. agencies, IATA or IOC, etc.).

Although all types of bribes and other inappropriate payments or conduct are prohibited under this Policy, JTB places a particular emphasis on interactions with Public Officials since the risk of engaging in corrupt behaviour involving Public Officials is much higher, and in many countries the penalties for such behaviours are generally heavier than similar bribes, inappropriate payments or conduct in respect of private persons or companies in many jurisdictions. It is also important to note that the FCPA, which has cross-border application, expressly prohibits corrupt behaviour involving even non-U.S. Public Officials.

B. No Use of Intermediaries for Prohibited Actions

All Employees are also prohibited from offering or paying Anything of Value to any person if it is known or there is a reason to know that all or part of such

payment will be used for the described prohibited actions set out at Section 2.A. above. This provision includes but is not limited to situations where intermediaries such as agents, consultants, and representatives are used to channel or redirect payoffs to Public Officials, private persons or companies.

C. No Excessive or Improper Gifts, Travel and Entertainment Expenses

(a) No Excessive Gifts or Offers of Entertainment

It may be customary in some countries to make small gifts or offer reasonable entertainment to a business counterparty or Public Officials in respect of the conduct of business. However, in general it is often difficult to judge the extent to which such gifts are customary and permissible. In addition, the global legal environment has become on the whole more severe and stringent with respect to such gifts even if they have been customary in certain countries. Such gifts are permissible so long as the gift is;

(i) Reasonable;

(ii) Necessary for conducting the business;

(iii) Not made corruptly to assist JTB in obtaining or retaining business; (iv) Made strictly in accordance with prior instructions by Management; and

(v) Legal in the relevant countries.

(b) No Payment of Unreasonable Costs

JTB may also pay for the cost of meals, lodging, or travel of a contract party (including both Public Officials, and private persons or companies) if the payment is;

(i) Reasonable;

(ii) Necessary for conducting business; and

(iii) Legal in the relevant countries.

The payment of such expenses is reasonable if the expenses are directly related to the promotion, demonstration, or explanation of JTB's product or services, or the execution of a contract with the contract party, and may legitimately be considered part of routine business travel and entertainment.

All Employees must be aware that payments for the expenses of a contract party that is not in the public sector (private persons or companies) are also subject to this Policy. In particular, the UKBA, which has cross-border application, prohibits bribery of both Public Officials and private persons or companies.

(c) Facilitation Payments

Facilitation Payments are small payments made to Public Officials, private persons or companies in accordance with publicly known or widely-followed local customs to expedite or secure the performance of routine government or private action, such as obtaining documents, processing governmental and/or procedural papers, or providing postal or utility services. JTB prohibits all Employees from making Facilitation Payments even in countries where the national law permits them.

3. IMPORTANT DUTIES OF EMPLOYEES

A. All Transactions Must Be Recorded In A Timely Manner

All transactions must be recorded in a timely and accurate manner in terms of amount, accounting period, accounting classification, description, and otherwise in accordance with the accounting policies adopted by JTB. No transaction shall be entered into that requires or contemplates the making or the receipt of false or fictitious accounting entries, whether unrecorded, recorded in whole or recorded in part.

B. Maintaining Awareness

It is the Employees' duty at all times to understand and comply with the Code and this Policy, as well as any internal procedures as described in Section 4.A. below. Failure to do so may result in disciplinary action up to and including termination of employment and in some countries the Employees in question may be personally and criminally liable.

C. Internal Reporting of Behaviour

Employees do not need to deal with issues of corruption alone. JTB is committed to taking appropriate steps to prevent and stop unlawful behaviour. However, this cannot be done without everyone's assistance.

Employees who suspect or believe that corruptive behaviour is occurring or has occurred shall immediately report the matter to the respective channel in accordance

with the internal reporting procedures described in Section 4.A. below. Employees who make reports based on their honest belief will not be subject to reprisal or have any damage done to their career, reputation or employment even if the subsequent investigation reveals that such report was wrong, or based on a misunderstanding.

4. RESPONSIBILITY OF MANAGEMENT

A. Establishment of Internal Procedures in Each Area of Operation

Management shall carry out reasonable investigations on the laws and regulations of each jurisdiction and identify the level of risk of corruption in each area of operation. Management shall establish proper mechanisms and procedures in each area of operation to prevent the occurrence of any corrupt behaviour by Employees. Such mechanisms and procedures shall include, amongst others, a secured reporting channel for Employees to raise concerns of any suspicious behaviour and detailed rules on the expenditure on or acceptance of gifts.

B. Communication of this Policy

Management shall also be responsible for ensuring that all Employees receive a copy of this Policy or always have access to it and are at all times in full understanding of the contents of this Policy, as well as any additional rules and procedures implemented in their own country and company.

C. Monitoring and Review of this Policy

Management shall monitor the internal mechanisms and procedures on an annual basis and at any time when they deem necessary to ensure that the Policy and the internal mechanisms and procedures are in accordance with updated applicable laws, regulations and the global trend in respect of the implementation and enforcement of anti-corruption laws.

Revision History

Version	Detail	Date
1.0	Newly established	2015/4/30
1.1	Updated in accordance with Japanese version 2018	2018/9/28
2.0	Updated in accordance with reestablishing JTB Group Policy	2023/4/1

Financial Policy

1. Commitments

(1) Commitment to accounting is to ensure appropriate financial reporting and to provide information that contributes to management's decision-making.
(2) Commitments to taxation is to ensure appropriate tax reporting and appropriate tax planning to maximize corporate value.
(3) Commitment to cash management is to ensure smooth business activities and effective use of cash in JTB group.

2. Definitions

(1) Implementation of appropriate financial reporting and provision of information that contributes to management's decision-making
①Appropriate accounting treatments
②Appropriate and timely disclosure of financial results
③Providing useful management information

(2) Proper tax reporting and appropriate tax planning to maximize corporate value
①Compliance with laws and regulations
②Build a firm relationships with tax authorities
③Optimize tax costs
④Minimize tax risks

(3) Smooth business activities and effective use of cash in JTB group
①Cash management based on safety, liquidity, and efficiency
②Foreign exchange transactions based on actual demand of the businesses

3. Details

(1) Implementation of appropriate financial reporting and provision of information that contributes to management's decision-making
①Appropriate accounting treatments
・The company always selects appropriate accounting principles, establishes these principles as rules, and implements accounting treatments based on these principles.
・ Integrate accounting treatments within JTB group, in general, for transactions of the same nature conducted in the same environment.
②Appropriate and timely disclosure of financial results

・Consolidated financial statements should be prepared by the deadline determined by the group on quarterly, interim, and yearly, in accordance with the "Principles of Consolidated Financial Statements" and other published rules, and report to the stakeholders.

③Useful management information

・Provide management information that is useful for effective implementation of management planning, management control, and other management controls.

・Always report accurate actual results and precise forecasting using the established methods by the deadline determined by the group .

(2) Proper tax reporting and appropriate tax planning to maximize corporate value

①Compliance with laws and regulations

・Compliance with laws and regulations of each country, tax treaties, and other international taxation rules.

②Build a firm relationship with tax authorities

・Establish an appropriate internal system to build trust with tax authorities and provide necessary cooperation in an appropriate manner.

③Optimize tax costs

・Carry out an appropriate tax planning to maximize corporate value, but will not engage in fraudulent tax avoidance.

④Minimize tax risks

・Tax risks in business activities are centrally identified and appropriately handled to minimize tax risks.

(3) Smooth business activities and effective use of cash in JTB group

①Cash management based on safety, liquidity, and efficiency

・Cash within JTB group will be visualized and managed centrally by the Treasury team.

・Using cash within JTB group is prioritized to meet the financial needs of the group.

・Surplus funds within JTB group shall be used efficiently by identifying the scope of risks.

②Foreign exchange transactions based on actual demand of the businesses

・Foreign exchange transactions within JTB group are managed centrally by the Treasury team.

・JTB group's foreign exchange risks are managed centrally by the Treasury team.

Revision History

Version	Detail	Date
1.0	Newly established	2023/4/1

PERSONAL DATA PROTECTION POLICY

1. COMMITMENT TO APPROPRIATE PROCESSING OF PERSONAL DATA

JTB has always placed and will place a priority on protecting Personal Data and individuals' right pertaining to Personal Data, regardless of whether it belongs to clients/customers, business partners or Employees. Leakage and/or loss of Personal Data as well as the mishandling of Personal Data can cause irrevocable damage to JTB and individuals.

With the increased use of computers for processing and dissemination of data, protection of Personal Data has become more important to maintain public trust and confidence in JTB; to protect the reputation of JTB; and to protect against legal liability for JTB. This Policy prohibits the use of Personal Data that violates applicable data protection laws and any JTB policy. JTB will take immediate and appropriate action in case of a violation of this Policy.

JTB WILL ALWAYS PROCESS PERSONAL DATA FAIRLY AND LAWFULLY. EACH AND EVERY EMPLOYEE IS RESPONSIBLE FOR UNDERSTANDING THE PROCEDURES TO HANDLE PERSONAL DATA APPROPRIATELY. EMPLYEES FOUND TO HAVE VIOLATED THIS POLICY (AFTER APPROPRIATE INVESTIGATION) MAY BE SUBJECT TO DISCIPLINARY ACTION UP TO AND INCLUDING IMMEDIATE TERMINATION OF EMPLOYMENT.

2. DEFINITION OF PERSONAL DATA

A. Definition of Personal Data

Personal Data (also known as Personally Identifiable Information or Personal Information in some jurisdictions) refers to any information relating to an identified or identifiable person (Data Subject), i.e., the information can be used on its own or in combination with other information to identify, contact, or locate a single person.

JTB recognizes that each country has different laws and regulations regarding Personal Data and that its definition also varies; there is no uniform and worldwide applicable definition. This Policy cannot address every possible detail regarding

the handling and use of Personal Data, but sets forth general rules on appropriate use thereof. This Policy sets forth the minimum guideline only; and if JTB and its business are subject to laws and regulations imposing more stringent obligations relating to Personal Data, JTB and its business shall comply with these obligations.

B. Examples of Personal Data

Examples of Personal Data include but are not limited to the following:

(i) Name;

(ii) Contact details such as telephone number, address, and e-mail addresses;

(iii) Personal details such as date of birth, age, sex, nationality, religion, marital status;

(iv) Personal identifiers such as identification card number (including but not limited to passport number, social security number, and driver's license number);

(v) Health records;

(vi) Criminal records;

(vii) Financial account details such as bank account details and credit card information;

(viii) Photos;

(ix) Other data that can identify a person.

Please note that the scope of Personal Data is not limited to only clients/customers but also that of business partners and Employees.

C. Sensitive Personal Data

In some jurisdictions, certain categories of Personal Data are defined as sensitive under the law. Examples of "sensitive" Personal Data in some jurisdictions are: health information, criminal record, race, ethnicity, gender, sexual orientation, political opinions, labour union membership, religious/philosophical convictions, and financial information, etc. All Employees should understand that additional, stricter rules might apply for the processing of "sensitive" Personal Data.

3. SCOPE OF THIS POLICY

This Policy shall apply to all Employees, who collect, use, disclose, transfer, modify, block, retain, record, process, organize, destroy, delete or otherwise have access to (collectively referred to as “process”) company-related Personal Data (during both working and non-working hours). It applies to Personal Data regardless of medium, e.g. contained in computer systems (e.g. computers, e-mails, communication devices) or hard-copies (e.g. documents in paper form). This Policy is internal to JTB and does not create any rights for Employees or third parties.

4. RESPONSIBILITY OF ALL JTB EMPLOYEES

All Employees shall comply with applicable laws, the following requirements and other instructions when processing Personal Data. In addition, each Employee shall comply with any procedures applicable specifically to his/her own business. When in doubt, Employees should check and consult with the company management ("Management").

A. Security and Accuracy of Personal Data

Employees shall take steps to reasonably protect Personal Data with care, using good judgment in accordance with this Policy and any additional applicable procedures issued pursuant to this Policy. Employees shall protect Personal Data against unauthorized processing.

(a) Limit Access to the Personal Data

Reasonable efforts should be made to limit the access of Personal Data only to Employees who require such information for legitimate business purposes such as providing products or services for which JTB is engaged or to otherwise fulfill the requirements of their role.

Employees shall not attempt to gain access to Personal Data that is not appropriate for their own role. If Employees come across such Personal Data accidentally, Employees shall not jeopardize the security or accuracy of the Personal Data.

(b) Securely store Personal Data electronically

Upon storing Personal Data electronically, Employees shall store it securely in accordance with this Policy whether on or off JTB business premises. Only company-issued or approved portable devices such as computers, laptops, tablets,

smartphones and information storage devices shall be used for work in general. Portable devices should not be left unattended.

Electronic files containing Personal Data shall always be protected with password. Password shall always be varied and no simple, easy-to-guess password shall be used. Employees shall limit the amount of Personal Data downloaded or saved on portable storage devices to what is absolutely necessary to complete work-related tasks/assignments.

(c) Store Hard-Copy Personal Data separately

Hard-copy documents containing Personal Data shall be stored separately from other documents in ways that limit inappropriate access such as storing them in locked cabinets or safes.

When handling hard-copy documents containing Personal Data, Employees shall never leave them unattended even within the office area. Leaving Personal Data unattended can result in loss or unauthorized access.

(d) Keep Accuracy of Personal Data

Employees shall take reasonable steps to maintain the accuracy of the Personal Data they process. For instance, some jurisdictions require that company provide contact information to the Data Subject to allow them to amend their Personal Data should the need arises.

B. Taking Personal Data out of the office

In some situations, Employees may need to take Personal Data out of the office for legitimate business purposes. During such occasions, Employees shall obtain permission from the Management and take only the Data and number of copies required, and ensure that they bring all the documents back to the office afterwards.

Employees who work remotely shall exercise the same care in protecting Personal Data as if they are working on-site in a JTB facility. Personal Data stored in paper form should be locked in a cabinet or safe and shredded upon disposal. Personal Data stored in computer systems shall be protected and secured with encryptions techniques approved by the applicable IT Section of each Regional Headquarters.

When discussing information containing Personal Data in public areas like hotel lobbies, restaurants elevators, in a train or an airplane, Employees shall ensure that Personal Data is not revealed to unauthorized third parties. This is also

applicable when Employees view Personal Data on a computer screen or hard-copy report in public places.

C. Transfer of Personal Data

Employees shall not transfer Personal Data outside of JTB or between JTB group companies unless the transfer is reasonably necessary for a legitimate business purpose. Prior to any transfer, Employees shall confirm that the transfer meets all required protections as established in any procedures advised by Management.

Upon transferring Personal Data electronically, Employees shall, as far as possible, not include Personal Data in the main body of an e-mail. Personal Data shall always be transferred with applicable safety measures, such as protecting the files with a password, or using encryption technology. Passwords shall never be sent together in the main body of the same e-mail but instead in a separate mail. Sharing the password in advance with recipients is another option. Company-related emails may not be forwarded to private email accounts or to any other non-work related e-mail address.

D. International Transfer of Personal Data

When transferring Personal Data electronically and non-electronically across national borders, Employees shall be aware of the legal restriction for the international transfer of Personal Data set forth in some jurisdictions regardless of whether transfer occurs within the JTB group companies or with external parties.

For example, the European Economic Area (EEA) basically does not allow any transfer of data to a third country (a country outside the EEA) unless that country ensures an “adequate” level of data protection. Many other countries, such as Australia, Hong Kong, India, Indonesia, Malaysia, Russia, Singapore, South Korea, Switzerland, and Taiwan also put some legal requirements for international transfers. Employees are requested to consult their Management for specific requirements in their own jurisdiction.

E. Destruction of Personal Data

Employees shall destroy Personal Data that are no longer required for legitimate business purposes securely in accordance with the applicable document retention policies. However, Personal Data subject to a legal or regulatory hold or other legal actions may not be destroyed. Employees shall consult their Management if they are unsure whether the Personal Data in question is subject to this requirement.

Electronic storage media containing Personal Data shall be destroyed or erased using methods approved by applicable IT Section in each Regional Headquarters. All hard-copy documents containing Personal Data shall be disposed by shredding or similar methods.

F. Reporting Incidents

Employees shall immediately report all incidents involving the suspected or actual loss, theft, unauthorized disclosure, or inappropriate use of Personal Data whether electronic or non-electronic, to the Management. In the event a third party processing company-related Personal Data notifies Employees of such an incident, Employees shall immediately report it to the Management. Employees shall also report the incidents involving the loss or theft of any company-related electronic device (even if no Personal Data is included in the device).

5. RESPONSIBILITY OF MANAGEMENT

In addition to the obligations set out in Section 4 above, Managements are also subject to the following obligations:

A. Determination of applicable laws

Managements shall define what is considered to be Personal Data pursuant to the applicable laws of each jurisdiction. They shall then determine if there is a need to further classify “sensitive” Personal Data and identify the necessary legal requirements to process “sensitive” Personal Data. Managements have to establish procedures for processing Personal Data according to specific industry requirements based on their definition.

B. Adhering to legal requirements

Where required by law, Managements shall appoint a Personal Data Protection Officer or an equivalent, notify data protection authorities and/or obtain approval from the competent data protection authority for the processing of Personal Data, and/or prepare documentation of data processing activities.

C. Processing of Personal Data

Managements shall ensure that Personal Data is processed in accordance with the applicable data protection laws. Where required by law, Managements shall establish procedures to explain to individual customers how their Personal Data is processed. Some jurisdictions have laws that require the following

information to be provided to Data Subjects upon collection of Personal Data (inter alia):

(i) The name of the company responsible for the Data processing ("**Company**");

(ii) The purposes for which the Personal Data is processed;

(iii) The categories of Personal Data and the categories of recipients to which the Personal Data may be transferred.

In addition, where required by law, Managements shall implement:

(i) Procedures to obtain Data Subjects' consent to the processing of Personal Data (some jurisdictions require express or implied consent for certain data processing activities, e.g. marketing activities, implementing cookies etc.).

(ii) Processes that allow individuals to access their Personal Data and amend inaccurate or incomplete Personal Data maintained by JTB; to object to the processing of Personal Data; or to withdraw consent for the processing of Personal Data.

D. Transfer of Personal Data to third parties

Managements shall establish procedures and set requirements for transferring Personal Data to third parties such as other JTB group companies and/or land operators, suppliers, and any other service providers who will process Personal Data on behalf of or for the respective JTB group company. These procedures and requirements have to ensure that the third party involved is bound legally by contract to (i) comply with all applicable privacy and data security laws and regulations; and (ii) to report immediately to the relevant JTB group company about any suspected or actual data security incidents (electronic or non-electronic) involving Personal Data. In addition, Management shall strive to bind the third party to (i) this Policy; and (ii) any procedures issued pursuant to this Policy.

E. International Transfer of Personal Data

Management shall establish procedures and requirements for transfer Personal Data to countries other than the country in which it was collected. As was set out in Section 4 above, some jurisdiction set forth the legal restriction for the international transfer of Personal Data.

These requirements may include but are not limited to:

(i) Company to obtain explicit consent from the Data Subject (which could include the express explanation about Data being disclosed to outside the jurisdiction and Company cannot guarantee same level of protection);

(ii) Recipient jurisdiction provides similar level of protection;

(iii) Company exercise due diligence to ensure that the Personal Data will be treated in accordance with the laws and regulation of the original jurisdiction;

(iv) Company entered into an appropriate data transfer agreement with the recipient;

(v) Company put into place binding corporate rules.

F. Thorough enforcement of procedures and rules

Managements shall also be responsible for ensuring that all Employees receive a copy of this Policy or always have access to it, and understand any additional rules and procedure implemented in their own jurisdiction and JTB group company.

6. MONITORING AND AUDITS

To evaluate compliance with applicable data protection laws and this Policy, the IT Section of each Regional Headquarters may, to the extent permitted by law, periodically monitor computer systems for unauthorized use of or access to Personal Data.

Revision History

Version	Detail	Date
1.0	Newly established	2015/4/30
1.1	Updated in accordance with Japanese version 2018	2018/9/28
2.0	Updated in accordance with reestablishing JTB Group Policy	2023/4/1

INFORMATION MANAGEMENT POLICY

This Information Management Policy ("**Policy**") sets out the procedures and processes that JTB has developed and implemented to ensure the proper use and management of JTB's information and assets in any JTB entities across the world, and the obligations required of JTB's officers, directors, employees and agents to ensure that all information and assets belonging to JTB, or that JTB may come into possession of in the course of its business operations, is managed and used in compliance with legal and ethical business requirements and regulations.

Policy consists of the following three policy.

1. Group policy of "Conflict of Interest"
2. Group policy of "Protection of JTB's Assets and Information"
3. Group policy of "Anti-Money laundering"

Group Policy of CONFLICTS OF INTEREST

1. Commitment of COFLICT OF INTEREST

(1) ALL DIRECTORS AND OFFICERS ARE RESPONSIBLE FOR AND MUST COMPLY WITH THE DUTIES AND OBLIGATIONS OWED TO JTB. JTB WILL NOT TOLERATE ANY MISUSE OR ABUSE OF POSITION BY DIRECTORS AND OFFICERS.

JTB RESERVES ALL RIGHTS TO TAKE ANY ACTION (LEGAL OR DISCPLINARY) AGAINST ANY AND ALL DIRECTORS AND OFFICERS THAT FAIL TO UPHOLD THEIR DUTIES AND OBLIGATIONS TO JTB.

(2) ALL PERSONNEL OF JTB MUST COMPLY WITH THE ANTI-CORRUPTION AND ANTI-BRIBERY OBLIGATIONS SET FORTH IN THIS POLICY.

WHERE A HIGHER STANDARD IS IMPOSED ON JTB BY ANY APPLICABLE LAW OR REGULATION, THAT HIGHER STANDARD MUST BE COMPLIED WITH.

2. Duties of Directors and Officers

In recognition of the fact that Directors and Officers of JTB are responsible for the management of JTB's business, certain duties and obligations are imposed on JTB's Directors and Officers to ensure that they discharge their responsibilities in an appropriate and lawful manner. These duties are as follows:

Table A: Duties of Directors and Officers

Duty	Extent and Scope
Duty Of Honesty and Diligence	Directors and Officers must at all times act honestly and exercise reasonable diligence in carrying out of their duties and responsibilities.
Duty To Act In The Best Interest Of JTB	In exercise of their duties, Directors and Officers must act in good faith in what they consider is in the best interests of JTB.
Proper Use Of Information And Position	Directors and Officers of JTB must not make improper use of any information acquired by virtue of their position with the company to gain, directly or indirectly, an advantage for themselves or for any other person or to cause detriment to JTB.
Duty To Exercise Powers For Proper Purposes	Directors and Officers of JTB must only exercise their powers for the proper purpose that the power was intended for.
Reliance On Advice	Directors and Officers of JTB may rely on the professional advice, reports, statements and other information of specific third parties who have the appropriate expertise or competence in the relevant matter. However, the Director and/or Officer must have: • acted in good faith in doing so; and • made any proper inquiries where such inquiry is warranted or required by the circumstances.

Conflict of Interest	Directors and Officers of JTB are obliged not to place themselves in a position where their duty to JTB may conflict with their personal interests. This is unless they properly disclose the conflict to JTB and obtain JTB's informed consent.

Directors and Officers are required to comply with the above duties.

3. JTB's Requirements of Its Directors, Officers and Employees.

3-1 Directors and Officers

In light of the above, JTB has set out below certain requirements which Directors and Officers must comply with:

（A） Directors and Officers must ensure that when making any decisions on behalf of JTB, they:

(i) make the decision in good faith for a proper purpose;

(ii) do not have a material personal interest in the subject matter of the decision;

(iii) inform themselves about the subject matter of the decision to the extent they reasonably believe to be appropriate; and

(iv) reasonably believe that the decision is in the best interest of JTB.

(B) Directors and Officers must not misuse their position to represent themselves as having the authority to bind JTB or execute agreements in JTB's name where such actions have not been approved by JTB's Board of Directors or with such persons with the relevant authority in JTB. All agreements must be approved in accordance with JTB's internal rules;

(C) Directors and Officers of JTB shall not place themselves in a position where their duty to JTB may conflict with their actual or potential personal interests (a "**Conflict of Interest**"). If Directors and Officers of

JTB find themselves in such a circumstance, they must notify JTB immediately;

(D) Directors and Officers of JTB must disclose any and all material personal interests, whether direct or indirect, in a transaction or proposed transaction that JTB may have entered or intends to enter into;

(E) Directors and Officers must not use their position to make a personal profit; and

(F) Directors and Officers must notify JTB of any commercial opportunities that they become aware of by virtue of their position.

The above obligations are in addition to the duties set out above in **Table A**, which all Directors and Officers of JTB are required to comply with.

3-2 Employees

Employees of JTB are required to comply with the terms and conditions of the employment handbook, as well as with all other applicable policies and guidelines as may be established by JTB from time to time.

Please note that in some jurisdictions, JTB may be found vicariously liable for the acts and omissions of its employees. Therefore, employees are also required to, when acting in their capacity as a representative and employee of JTB, act prudently and in the best interests of JTB. This would mean complying with the following obligations:

(A) Employees must not misuse their position to represent themselves as having the authority to bind JTB or execute agreements in the JTB's name where such actions have not been approved by JTB's Board of Directors or with such persons with the relevant authority in JTB. All agreements must be approved by JTB's Board of Directors or the relevant person, where applicable, before they are executed;

(B) Employees shall not place themselves in a position where there is a Conflict of Interest. If employees find themselves in a Conflict of Interest in the course of carrying out their duties, employees must inform their manager immediately;

(C) Employees of JTB must disclose any and all material personal interests, whether direct or indirect, in a transaction or proposed transaction that JTB may have entered or intends to enter into;

(D) Employees must not make a personal profit in the course of carrying out their activities; and

(E) Employees must notify JTB of any commercial opportunities that they become aware of in the course of carrying out of their duties.

4. Anti-Corruption and Anti-Bribery

JTB is firmly committed to maintaining the highest standards of ethics and has a zero-tolerance towards bribery and corruption. JTB prohibits all forms of bribery and corruption, as well as any business conduct that could create the appearance of bribery and corruption. JTB's commitment to this cause requires strict compliance with all applicable laws, prohibiting improper payments, gifts or inducements of any kind to and received from any person, including officials in the private or public sector, clients/customers and suppliers.

In this regard, JTB has developed and established the Anti-Corruption Policy which sets out JTB's policy on anti-bribery and anti-corruption, as well as the compliance obligations, duties and procedures that all of its personnel, including its Directors, Officers, employees and agents (collectively, "**Personnel**") are required to abide by in the conduct of their business.

Please note that where an applicable anti-bribery and anti-corruption law or regulation in a specific country imposes a higher standard of compliance, the JTB entity and its Personnel in that country shall comply with that higher standard.

Please note that failure to comply with the Global Anti-Corruption Policy may result in criminal liability for both the individual and JTB. Therefore, Personnel of JTB must ensure that all relevant compliance obligations, duties and procedures are complied with.

4-1 Anti-Corruption and Anti-Bribery Obligations

JTB strictly prohibits all forms of bribery, corruption or other improper payments or gratifications in any of its business. All Personnel of JTB are required to comply with the same.

4-2 Reporting Possible Violations

Any Personnel of JTB who is aware of, or has reason to believe that, the above bribery policy has been infringed or violated, may report such an infringement or violation to JTB in accordance with the procedures set out in the Anti-Corruption Policy. Retaliation against any Personnel of JTB that has made a bona fide report of an infringement or violation, or possibility thereof, is strictly prohibited.

5. Disclosure Procedures

5-1 Conflicts of Interest

Any disclosures of Conflicts of Interest, whether actual or potential, or of any commercial opportunity that Directors, Officers and employees may become aware of as by virtue of their position must be made to the relevant persons in JTB.

For employees, such information must be disclosed to their managers.

For Directors and Officers, such information must be disclosed to JTB's Board at a general meeting.

Such disclosures must contain sufficient detail to allow the relevant person to whom the disclosure is made to:

(A) identify the personal interests in question, and the identity of any other person(s) or entit(ies) that is connected to the Director, Officer or employee to whom such interests relates;

(B) identify the nature of the conflict and its implications and consequences, whether actual or potential, on JTB;

(C) identify whether any business relationships or transactions may be affected by the conflict;

(D) identify whether JTB is likely to suffer any damage or loss; and

(E) make a decision whether JTB may provide its approval (where sought) or if JTB needs to take any further action.

Should JTB decide that a further investigation is necessary, all Directors, Officers and employees shall provide any and all necessary assistance and information to enable JTB to conduct such investigations.

5-2 Disclosure of Gifts and Favours

Any gifts or favours offered or accepted by Personnel of JTB must immediately be disclosed to his/her manager in accordance with the reporting procedures set out in JTB's Global Anti-Corruption Policy.

PROTECTION OF JTB'S ASSETS AND INFORMATION

1. Commitment of PROTECTION OF JTB'S ASSETS AND INFORMATION

ALL PERSONNEL OF JTB MUST COMPLY WITH REQUIREMENTS SET OUT ABOVE IN RELATION TO THE PROTECTION OF JTB'S ASSETS AND INFORMATION.

JTB RESERVES ALL RIGHTS TO TAKE ANY ACTION (LEGAL OR DISCPLINARY) AGAINST ANY AND ALL PERSONNEL WHO FAIL TO COMPLY WITH THE ABOVE OBLIGATIONS AND/OR TO RECOVER ANY LOSS, DAMAGE OR LIABILITY THAT RESULTS FROM A BREACH OF THE ABOVE OBLIGATIONS.

2. Classification of JTB'S Information

JTB has established the following classifications for information and data belonging to JTB:

Table B: Information and Data Classification

Classification	Description
Confidential	Information and data which are commercially valuable and/or sensitive to JTB, and which value is dependent on its confidentiality, such that any unauthorised disclosure of such information or data may result in JTB being unable to take advantage of such information or data any longer, or in JTB suffering significant pecuniary loss or damage, or which may result in JTB being the subject of any potential lawsuit. Confidential Information shall only be disclosed to and accessible by JTB's Personnel that have been **specified and authorised** by JTB. Some examples of Confidential Information include trade secrets, undisclosed inventions, proprietary information, client, supplier and customer lists, business plans and marketing strategies, information relating to proposed transactions which are currently being negotiated on etc...
Restricted	Information and data apart from those classified as "Confidential Information" which are for use within JTB only and which need to remain confidential as any unauthorised disclosure of such information or data may result in pecuniary loss or damage to JTB, or which may result in JTB being the subject of any potential lawsuit. Restricted Information shall only be disclosed and shared on a need-to-know basis with authorised Personnel or classes of Personnel (such as on a department level). Some examples of Restricted Information include internal memos, personal data of employees, information which JTB is under confidentiality obligations.

Internal	Information and data which are intended for use within JTB only and which unauthorised disclosure may be prejudicial to JTB's interests. Internal Information shall be made available to all Personnel of JTB. However, such information is not intended to be shared with any third parties. Some examples of Internal Information include JTB's internal policies and procedures.

The relevant persons who are in charge of general administration or other persons designated by JTB ("Information Controllers") shall be responsible for classifying information and data into the categories set out above in **Table B** according to the level of confidentiality commensurate to the nature and importance of such information or data.

3. Data Protection Obligation

The protection of JTB's information and data is the responsibility of all JTB Personnel. All JTB Personnel are required to comply with any directions or instructions given by the Information Controllers.

Certain jurisdictions also impose additional responsibilities on JTB regarding the collection, use and/or disclosure of data which can identify individuals, directly or indirectly with other data to which JTB has or is likely to have access ("**personal data**"). As a baseline standard, JTB expects all of its Personnel, in any jurisdiction, to comply with the personal data protection standards that it has developed and established. Please refer to JTB's Personal Data Protection Policy for more information on such personal data protection standards and obligations.

4. Data Administration Guidelines

4-1 General

Upon the creation or receipt of any information or data, and at any time as may be necessary, the Information Controllers shall review the nature of the information and classify it within the categories set out above. All Personnel of JTB are expected to assist the Information Controllers in his

/ her aforementioned duties by notifying him / her, and no one else, of the creation or receipt of any information and data which may be relevant or which may need to be reviewed for classification, as soon as such information is created or received.

Additionally, where any information constitutes personal data, the Information Controllers shall take steps to verify that:

A. the individual to whom the personal data relates has been notified of the purposes for the collection, use and/or disclosure of his / her personal data by JTB;

B. the individual has consented to the collection, use and/or disclosure of his / her personal data by JTB for such purposes;

C. that the information provided is accurate and complete; and/or

D. such other requirements as set out in the Personal Data Protection Policy iscomplied with.

For information classified as “Confidential” or “Restricted”, the Information Controllers shall also:

A. specify the authorised Personnel, or classes of Personnel within JTB, to which the information may be shared, disclosed or accessed;

B. provide instructions on how such information should be handled, protected or managed by the aforementioned authorised Personnel;

C. implement, or require the authorised Personnel to implement, necessary security measures to prevent the unauthorised disclosure of the information, such measures may include but shall not be limited to encryption of the information, placing the appropriate markings and labels of confidentiality such as “Strictly Confidential” and ensuring that hard copies are kept securely in locked storage; and

D. impose such conditions for the access and use of such information, including requiring any authorised Personnel to sign a non-disclosure agreement or a confidentiality undertaking.

The Information Controllers shall review all JTB's information periodically to assess whether any change in the classification is required. In addition, the Information Controllers may revoke the access of Classified Information to any authorised Personnel at any time.

4-2 Use of Classified Information

Authorised Personnel shall only use Classified Information for the purposes for which access to the Classified Information was given to the authorised Personnel and in compliance with any conditions or instructions that apply to the access to and use of such Classified Information. Failure to comply with this obligation may result in disciplinary action, after proper due inquiry is conducted, against the relevant Personnel and/or such access rights being revoked, as well as such other statutory, contractual and/or equitable remedies which JTB may pursue against the relevant Personnel for such a failure to comply with this obligation.

4-3 Disclosure or Sharing of Classified Information

Authorised Personnel shall not disclose or share any information classified as "Confidential", "Restricted" or "Internal" (collectively, "**Classified Information**") with any third parties (including other Personnel of JTB not authorised to access or receive such Classified Information or any external third parties) without the prior written approval of the relevant Information Controllers. The Information Controllers may, prior to giving any written approval, impose any conditions for the disclosure or sharing of such Classified Information. No information classified as "Confidential" or "Restricted" shall be disclosed or shared with any external third party without the external third party agreeing to be subject to a confidentiality agreement or a non-disclosure agreement which shall set out the obligations of confidentiality and the consequences for a breach of the same.

4-4 Return or Destruction of Classified Information

Upon notice of the termination or resignation of any Personnel, or where access rights to any Classified Information has been revoked by the Information Controllers, all access to and use of the Classified Information (if any) by the relevant Personnel shall cease and the relevant Personnel must comply with the same.

Additionally, the relevant Personnel shall, without further delay, destroy and/or return, at JTB's sole and absolute discretion, all Classified Information in his /her possession and/or under his/her control to JTB, and cease to retain any such Classified Information. JTB may request that the relevant Personnel certifies in writing, by way of a statutory declaration for Directors and Officers of JTB, and a written undertaking for employees of JTB, that the relevant Personnel has complied with the aforementioned obligations and that, to the best of his/her knowledge, he/she no longer retains in his/her possession and/or under his/her control, any Classified Information.

The Information Controllers shall be entitled to conduct a check to ensure that the relevant Personnel has destroyed or returned all Classified Information to JTB, and all Personnel must provide their fullest cooperation and assistance to the Information Controllers conducting such a check. This includes, without limitation, allowing JTB to conduct an exit interview and/or allowing the Information Controllers to access the relevant Personnel's personal devices, computers, lockers, and other storage devices, mediums or items, whether for the storage of Classified Information in hard copy or in electronic form.

5. Proper Management and Use of JTB's Assets and Information

5-1 Proper Management and Use of JTB's Information

JTB's information shall be used, managed or disclosed for legitimate purposes related to JTB's business operations, only with the permission of the Company, and in the exercise of the Personnel's duties. Authorised Personnel shall only use Classified Information for the purposes for which access rights were granted to the authorised Personnel, and in compliance with any conditions or instructions that apply to the access to and use of such Classified Information.

All Personnel are required to maintain the confidentiality of all Classified Information that is or that may reasonably be expected be assumed to require its confidentiality to be maintained, both during and after their employment with JTB for any reason whatsoever.

All Personnel are prohibited from contacting the media or responding to inquiries

Without the permission of the department that deals with the media,if there are inquiries from the media.

All Personnel are required to comply with the applicable Data Administration Guidelines, set out above in **Section 4** of this Policy, in relation to their use, management or disclosure of JTB's information.

JTB reserves the right to take any action necessary to protect the confidentiality of its information and / or to recover any loss, damage or liability that results from any Personnel's failure to comply with his / her obligations under this section, including the obligation to use and manage the information for the proper purpose that it was intended for and any obligations of confidentiality.

5-2 Proper Management and Use of JTB's Assets

In each jurisdiction, JTB may own certain assets and property, including but not limited to physical assets such as real estate (office premises / buildings, stores) and movable property (office stationery, computers and other IT equipment, goods and products), and intangible assets such as information of a classified and confidential nature and intellectual property rights.

JTB assets are to be used only for legitimate or authorised purposes related to
JTB's business operations. Any misappropriation or damage to JTB's assets and / or any unauthorised or improper use of JTB's assets are strictly prohibited. In particular, all Personnel must not use, divert or appropriate JTB's assets, for personal use or benefit. The improper and unauthorised use of any of these will be treated as theft.

If any Personnel is found to have misappropriated or damaged JTB's assets or to have used JTB's assets for an unauthorised or improper purpose, the appropriate disciplinary action will be taken against the relevant Personnel after proper due inquiry is conducted. Notwithstanding this, JTB reserves the right to commence civil proceedings to recover any loss or damage suffered by JTB as a result of the relevant Personnel's actions, or to report the relevant Personnel to the appropriate authorities where the relevant Personnel's act constitutes a criminal offence.

If any Personnel becomes aware of any misappropriation, damage or unauthorised use of JTB's assets, that relevant Personnel must alert the relevant Information Controllers and / or the Legal Department immediately.

5-3 Proper Use of IT Systems

JTB provides its Personnel with access to and use of certain Information Technology Systems ("IT Systems") which include, but is not limited to, internet and intranet access, networks and servers, strictly to enable its Personnel to perform their duties in relation to JTB's business operations.

All Personnel shall only use JTB's IT Systems for legitimate or authorised purposes related to JTB's business operations. All Personnel should not attempt to access or use JTB's IT Systems for any improper or unauthorised purpose(s), or to gain unauthorised access to external IT Systems.

Please refer to JTB's Global IT Security Handbook for more information.

If any Personnel is found to have misused JTB's IT Systems, or to have accessed or used or attempted to access or use JTB's IT Systems for an improper or unauthorised purpose, the appropriate disciplinary action will be taken against that Personnel after proper due inquiry is conducted. Notwithstanding this, JTB reserves the right to commence civil proceedings to recover any loss, liability or damage suffered due to or resulting from the relevant Personnel's actions, or to report the relevant Personnel to the appropriate authorities where a criminal offence has been committed.

If any Personnel becomes aware of any security breach in the JTB's IT System, or of any unauthorised access or use of the same, he / she must alert the relevant Information Controller and / or the IT Department immediately.

6. Restrictions on Insider Trading

JTB may, in the course of its business operations or of any mergers, takeovers, amalgamations or joint ventures, come into possession of

sensitive information relating to JTB or other companies that may be relevant to or listed on a public stock exchange.

Such sensitive information includes any information that is not generally available to the public, but if the information were generally available, a reasonable person would expect it to have a material effect on the price or value of securities or of share prices on a public stock exchange. Examples would include information about an imminent merger and acquisition, or takeover.

In such an event, JTB and its Personnel must take care in the way that they deal with such sensitive information.

Certain jurisdictions contain laws prohibiting or restricting insider trading, a violation of which may result in criminal and civil liability for both JTB and the individual. As a baseline standard, JTB strictly prohibits all of its Personnel from conducting any activities which may constitute insider trading. For the avoidance of doubt, sensitive trading shall constitute:

A. subscribing for, purchasing or selling, or entering into any agreement to subscribe for, purchase or sell, any such securities or shares related to the sensitive information;

B. procuring another person to subscribe for, purchase or sell, or enter into an agreement to subscribe for, purchase or sell, any such securities related to the sensitive information; or

C. sharing such sensitive information with any third party.

ANTI-MONEY LAUNDERING ("AML")

1. Commitment of ANTI-MONEY LAUNDERING

JTB is required to comply with various requirements and regulations relating to anti-money laundering, reporting of suspicious transactions, and the prevention of terrorism financing.
All Personnel of JTB shall render their full cooperation and assistance to ensure that JTB complies with any anti-money laundering requirements and regulations that may be applicable to it.

JTB reserves all rights to take any action (legal or discplinary) against any and all personnel who fail to comply with the above obligations and/or to recover any loss, damage or liability that results from a breach of the above obligations.

2. Definition of Suspicious Transactions

Generally, a "suspicious transaction" refers to any transaction in which any property, including but not limited to funds or money, that is, or is suspected to be, directly or indirectly connected to any criminal conduct, is handled, managed in the course of, or otherwise the subject of the transaction.

Some obvious examples are where the payment of funds is from an account that is known to belong to a criminal organisation, syndicate and/or terrorist group. Other examples include the payment of funds from anonymous accounts or sources, or from countries which are sanctioned or which are placed on high risks lists, where the client's identity cannot be verified through the necessary due diligence and verification measures, or where the transactions cannot be reconciled with the usual business activities of the client.

All Personnel of JTB are required to refer to the anti-money laundering authority and/or suspicious transaction reporting office in the relevant jurisdictions to ascertain whether there are any inconsistencies or additional "red flags" or indicators that exist and that JTB should take note of. Where such an inconsistency exists, the definition of suspicious transaction as specified by the relevant anti-money laundering authority

and/or suspicious transaction reporting office shall prevail over this Policy to the extent of the inconsistency.

3. Prohibited Business Relationships

JTB shall refuse to enter into a business relationship with, or to provide its services to, and shall cease any business relationships with, or the provision of any of its services to, any clients, whether individuals or entities that:

A. are known to be, or reasonably suspected to be, members of and/or related to any criminal organisation, syndicate and/or terrorist group;

B. are from countries specified in a sanctioned list and/or otherwise highlighted as being of a special risk; and/or

C. have been otherwise placed on a sanctioned list or such other restricted list in the relevant jurisdiction.

JTB shall comply with the above obligations where it cannot, through any due diligence or verification measures set out herein or as may be undertaken by JTB from time to time, verify whether the client or potential client belongs or does not belong to a category set out above.

All personnel of JTB shall render their full cooperation and assistance in complying with JTB's obligations set out above.

4. Know Your Client – Verification Measures

JTB has established a baseline standard to comply with applicable Know-Your Client Requirements. Where any applicable laws or regulations in a jurisdiction impose a higher standard of compliance, JTB shall comply with that higher standard.

Under this Policy, a client of JTB refers to:

(a) a person or entity that enters into a transaction or which has a business relationship with JTB;

(b) a person or entity on whose behalf the transaction or business relationship is entered into (i.e. a beneficial owner); and/or

(c) any other person or entity connected to the transaction which may result in JTB being in breach of its compliance requirements under any applicable laws or regulations in the relevant jurisdiction.

4-1 KYC Verification Measures

As far as possible, JTB shall, prior to entering into a business relationship or a transaction with a potential client, take the following verification measures:

- 4-1-1 **Verification of Client Identity**

JTB shall request for the following information, as well as for supporting documents to verify the information, from the client:

i. Full details of the client (including full name or registered business name, address etc…);
ii. Nationality (if client is an individual) or country of incorporation/registration (if the client is a corporate entity); and
iii. Whether there is any beneficial owner and if so, further details about the beneficial owner (which shall match those set out above).

Where possible, JTB shall also search public registries to ascertain and verify the identity of the client.

If, based on the information provided above by the client, JTB has reason to suspect that a transaction or business relationship with the client may be prohibited under this Section, JTB shall seek the following further information:

i. Information about the source of funds, where possible; and
ii. Where the client is a corporate entity, the identity and details of all connected parties and natural persons who act on behalf of the entity.

JTB shall only proceed with the transaction or business relationship after it has verified the client's identity and is satisfied that a

transaction or business relationship with the client may be prohibited under this Section.

- 4-1-2 **Collection and Retention of Client Information**

  JTB shall collect and retain, for its record keeping purposes, all of the aforementioned information, as well as the nature, volume and frequency of any transactions a client may have with JTB, on an ongoing and periodic basis and as may be necessary.

- 4-1-3 **Monitoring, Updating and Reporting of Client Information**

  JTB shall monitor and update the aforementioned client information to ensure that it is as accurate and up to date as reasonably possible.

  JTB shall also monitor transactions and other business activities of the client and report such transactions which are suspicious, or which may be indicative of illegal activities.

Where it is not possible to complete the KYC verification measures set out above before the business relationship or transaction is entered into, JTB shall conduct the KYC verification measures as soon as reasonably possible.

JTB shall, as far as is practicable, conduct the above KYC verification measures by itself. However, where permissible under the laws and regulations of a relevant jurisdiction, JTB may engage such third parties to assist JTB in conducting the above KYC verification measures.

All Personnel shall ensure that it complies with the obligations set out above.

5. JTB's Compliance and Suspicious Transactions Reporting Process

JTB's position is that all suspicious transactions must be reported to the relevant anti-money laundering authority and/or suspicious transactions reporting office.

Any Personnel who is aware of, or has reason to believe, that any transaction is one that constitutes a suspicious transaction, shall

immediately report the same to Information Controllers. The Information Controllers shall then work together with the relevant Personnel to file the suspicious transaction report in accordance with any requirements and/or forms as may be set out in the relevant jurisdiction. This includes complying with any obligation or requirement to provide any mandatory details as may be required under the relevant laws and regulations of that jurisdiction.

Where the anti-money laundering authority and/or suspicious transactions reporting office of a relevant jurisdiction prescribes a particular form or template on which to make the report, JTB and its Personnel shall comply with that form or template.

JTB and its Personnel shall monitor and review all transactions and business relationships on an ongoing and periodic basis to ensure that JTB is in compliance with any applicable regulations and laws relating to anti-money laundering, reporting of suspicious transactions and the prevention of financing of terrorism.

JTB and its Personnel shall also keep a list of transactions and clients that are of a high risk of falling within the scope of Prohibited Business Relationships within this Section and shall ensure that particular attention is given to such transactions and clients, and that the same are monitored and reviewed on regular basis at a greater frequency.

Revision History

Version	Detail	Date
1	Newly developed	30 June 2016
2	Revised	1 April 2023

[*End of Policy*]