SUNTORY

Suntory Group Supplier Guidelines

Purpose

In order to provide high-quality products and services safely and reliably based on our corporate philosophy "To Create Harmony with People and Nature" and "Growing for Good", as well as our Suntory Group Code of Business Ethics, the Suntory Group, as a signatory to the United Nations Global Compact, engages in fair business practices and, in collaboration with supply chain business partners, promotes procurement activities that take social responsibility into consideration, mindful of such points as human rights, labor standards, and the environment. We build good partnerships with our business partners and contribute toward realizing a truly affluent and sustainable society.

These Suntory Group Supplier Guidelines are intended to set the principles of Suntory Group companies to the network of suppliers of the Suntory Group. The Suntory Group Supplier Guidelines provide the basic principles that suppliers of the Suntory Group (hereinafter called "Suppliers") shall respect, but also emphasize that engagement between both the Suntory Group entity and its Suppliers is essential to achieve a sustainable supply chain. It is the first step of the approval process before any commitment with the Suntory Group. This commitment ensures that the Suntory Group and the Suppliers share the same ethical values which are the first key step of any successful relationship.

To comply with all our requirements, Suppliers are expected to engage their own partners, supply chain and subsidiaries to respect the Suntory Group Supplier Guidelines. Suppliers must comply with international, national and industry related legislations where they operate. The Suntory Group encourages Suppliers to go beyond legal compliance and to work on continuous improvement.

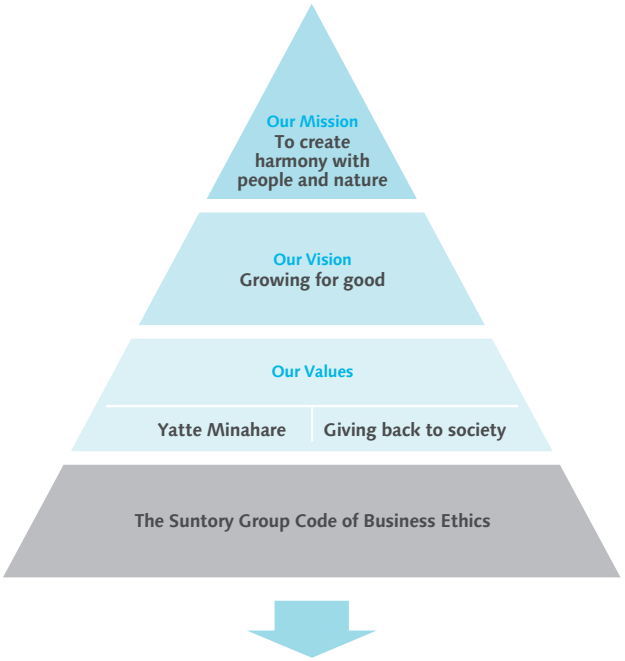
Corporate Philosophy page :
http://www.suntory.com/about/philosophy/

Basic Policy on Supply Chain CSR page :
http://www.suntory.co.jp/company/csr/activity/service/procurement/

Corporate Tagline

SUNTORY
FOLLOW YOUR NATURE

The Suntory Group Philosophy



The Suntory Group's Basic Policy on Supply Chain CSR

1. Legal Compliance and Respect for International Standards of Conduct
We will promote fair and equitable procurement activities that comply with each country's laws and respect international standards of conduct.

2. Consideration for Human Rights, Labor, and Safety and Health
We will promote supply chain CSR initiatives that respect basic human rights and are mindful of labor conditions and safety and health.

3. Guaranteeing Quality and Safety
In keeping with the Suntory Group Quality Policy, we will promote supply chain CSR initiatives that seek to guarantee a high level of quality and safety based on the optimal standards for quality, cost, and supply.

4. Consideration for the Global Environment
In keeping with the Basic Principles of Suntory Group's Environmental Policy, we will promote procurement activities mindful of the global environment.

5. Preservation of Information Security
Proprietary information regarding procurement dealings and personal information will be strictly controlled.

6. Coexisting within Society
We will promote social contribution initiatives directed toward coexisting within society.

Suntory Group Supplier Guidelines

1. Legal Compliance and Respect for International Standards of Conduct

Business Integrity
Suppliers must avoid any type of fraudulent practices including conflict of interest, extortion, money laundering, etc.

Bribery and corruption
Suppliers must avoid any type of bribery and corruption and comply with all applicable laws.

Fair Competition and anti-trust
Suppliers must demonstrate fair business practices and must comply with all relevant anti-trust laws and regulations.

Gifts and entertainment
Suppliers are expected to not provide or accept excessive or inappropriate gifts and/or entertainment and only offer or accept gifts occasionally and that are of modest value.

Reporting concerns
Suppliers are expected to have appropriate mechanisms by which employees can raise concerns protected from retaliation.

2. Human Rights, Labor, and Safety and Health

Child labor
Suppliers must prevent child labor and comply with all applicable child labor laws, including the International Labor Organization (ILO) standards.

Forced labor
Suppliers must prevent involuntary labor and any form of human trafficking.

Working hours
Working hours must comply with all local laws and regulations, ILO standards and/or collective agreements.

Wages and benefits
Wages and benefits must be in line with local legislation and meet or exceed the legal minimum standards of the country where the workers are employed.

Non discrimination
Discrimination in hiring and employment practices must be prohibited on the grounds of race, religion, sex, age, nationality, language, disability or any other status protected by all applicable laws.

Abuse and harassment
The threat or use of physical abuse and/or discipline must be prohibited along with any other forms such as verbal, psychological or sexual abuse.

Freedom of association and collective bargaining
Suppliers must respect the right of employees to freely associate, organize and bargain collectively in accordance with applicable laws.

Access to remedy
Suppliers must provide a right to remedy for their employees through an accessible and fair grievance process.

Health & safety policy
Suppliers must have a health & safety policy, identify any hazards in the workplace, manage them and communicate any potential dangers to the employees.

3. Product Quality and Safety

Product quality
Suppliers must follow all applicable regulations, and quality delivered must meet approved specifications as agreed by both Suntory Group Companies and Suppliers (hereinafter called "parties").

Product safety and regulations
Suppliers must keep themselves constantly informed and respect all legal requirements, deriving from national, of country of manufacture and material destination, and international regulations regarding products and their manufacture.

Transportation
Transportation must comply with the Suntory Group standards as agreed by both parties, including container inspection, pallet treatment to prevent taint and/or objectionable odor. At no point during transportation should the product be susceptible to any contamination.

Provision of reliable product information
Suppliers must guarantee that the product or service they deliver respects all Suntory Group specifications and must provide related documentation as agreed by both parties.

Crisis Management and stable product supply
In the event where a failure to supply a Suntory Group company is apparent, and where business continuity is to be impacted as a result, Suppliers must contact that Suntory Group company so that a contingency measures can be agreed and implemented.

4. Global Environment

Environmental management
All systems are expected to be in place to respect the law so that Suppliers comply with local legislation on environmental issues, and the adoption of global standards such as ISO 14001 is encouraged.

Waste Management
Suppliers are expected to implement plans to reduce waste as much as possible. Controls must be in place and hazardous waste should be treated separately and handled carefully according to procedures implemented. Where possible, recycling of waste is emphasized.

Water Management
Suppliers are expected to control the use of water in all its activities, reduce its use as much as possible and ensure that there is no release of waste water directly into nature. Engagement on the conservation of water resources in order to achieve a sustainable use of water is encouraged.

Energy Usage
Suppliers are expected to implement plans to reduce greenhouse gas emissions as much as possible, using methods such as the use of renewable energy where possible. Energy reduction plans are encouraged.

Environmental pollution
Suppliers must demonstrate legal compliance and good practice in the management of pollution to land, air or water.

Biodiversity
Suppliers must demonstrate legal compliance and good practice if operation of their business may potentially impact biodiversity.

5. IT Security and Data Protection

Computer Network Threats
Suppliers are expected to put in place measures aimed at protecting computer networks against threats.

Confidentiality and Personal Data Protection
Suppliers must safeguard and protect confidential and personal information of all business partners, third parties, employees, and other individuals and organizations and must comply with all related applicable laws.

6. Coexisting within Society and Nature

Contributing to Society and Local Community

Suppliers are encouraged to voluntarily engage in activities that contribute to the growth and development of the international and local communities.

Encouraging Sustainable practices

Suppliers are encouraged to voluntarily engage in/promote sustainable practices so as to ensure precious global resources such as water and agricultural products for future generations.

The Suntory Group or appointed representatives of the Suntory Group companies have the right to access partner's factory/ premises to check quality (products and process), human rights, environmental aspects and ethical compliance if necessary. Suppliers must be open and provide all information related to its business with the Suntory Group.

Suntory MONOZUKURI Expert Limited
Supply Chain Management Division

Suntory Holdings Limited
Corporate Communication Division

(Established in June, 2017)

SUNTORY

FOLLOW YOUR NATURE

SUNTORY
OCEANIA

Modern Slavery and Data Protection Schedule

February 2025

Modern Slavery

Defining Modern Slavery

The nature and extent of modern slavery means there is a high risk that it may be present in Service Providers' operations and supply chains. Modern slavery has a broad scope and includes practises involving slavery or slavery like offences, forced labour, deceptive recruiting for labour or services, forced marriage offences, debt bondage, threats of coercion, trafficking in persons and/or children, organ trafficking, and harbouring a victim.

Commitment to Human Rights and Modern Slavery

The Suntory Group is committed to ensuring there is transparency in its operations and approach to tackling modern slavery and to preventing, detecting, and reporting on the risk of slavery or human trafficking in operations and supply chains.

Compliance with laws and standards

Service Providers must comply at all times with Modern Slavery Laws. Service Providers must not do or omit to do anything that will cause the Suntory Group to breach Modern Slavery Laws.

Modern Slavery Laws means any primary or delegated/subordinate legislation and amendment (and any binding or non-binding guidelines issued by any entity or person so authorised under Modern Slavery Law), applicable in Australia, any State or Territory and/or otherwise applicable to the Suntory Group or its Service Providers from time to time with respect to reporting on and/or addressing the risks of Modern Slavery, including in business operations and supply chains and with respect to related purposes including but not limited to:

a. Fair Work Act 2009 (Cth);
b. Modern Slavery Act 2018 (Cth);
c. Modern Slavery Act 2018 (NSW);
d. Criminal Code Act 1995 (Cth), specifically, Division 270 or 271 of the Criminal Code, extending to conduct in and outside of Australia;
e. Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework;
f. Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; and
g. ILO Convention (No. 182) concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour.

Requirements

Service Providers must take adequate measures to prevent, mitigate and remediate the risk of modern slavery occurring in internal operations and supply chains.

Service Providers must comply with any reasonable requests the Suntory Group may make for assistance and/or information to aid in the review of compliance with this Appendix.

Service Providers must ensure:

a. All recruitment and on-boarding processes are ethical and legally compliant;

b. All staff are provided with a written contract relevant to the work they are undertaking which expressly provides for the wage, working hours and employment conditions of that contract. These contracts should be in a language that the staff member understands; and

c. All staff are provided with a safe, accessible and hygienic working environment.

Reporting and Breaches

Non-compliance with this Appendix will be taken very seriously. Service Providers must monitor their own compliance with this Appendix and notify the Suntory Group within 14 days of becoming aware of any breach or potential breach of the Appendix by the Service Provider or any of its staff.

Agencies or individuals who suspect that any individual, group, or entity is acting in breach of this Appendix can contact the whistle blowing hotline on 0800 ON WATCH to report the matter. Agencies must treat such disclosures in accordance with Whistleblowing laws.

Referral action to proper authorities may be taken in cases involving breaches of criminal law.

Privacy and data protection requirements

1. BACKGROUND

Subject to the terms of this Schedule, the Service Provider may use Principal Data in connection with this Agreement. Accordingly, the Service Provider undertakes that it will comply with the specific obligations relating to Principal Data set out in this Schedule.

2. DEFINITIONS AND INTERPRETATION

2.1. DEFINED TERMS

For the purposes of this Schedule, unless the context otherwise requires:

a. Agreement means the agreement between Principal and the Service Provider to which this Schedule is attached.

b. Data Breach means any unauthorised or accidental access to, or disclosure, alteration, interference, misuse, loss, or destruction of, Principal Data, or any action that prevents the Service Provider from accessing Principal Data on either a temporary or permanent basis.

c. Principal means Principal New Zealand Limited and Principal Australia Pty. Limited, and its related companies or related entities.

d. Principal Data means all Personal Information about Principal's customers and/or employees,

   i. provided to the Service Provider by or on behalf of Principal, and/or

   ii. used by the Service Provider in the course of providing any goods and/or services to Principal.

e. Personal Information has the meaning given to that term in the Privacy Act 2020 (NZ) or the Privacy Act 1988 (Cth) (as applicable).

f. Purpose(s) means for the purpose of the Service Provider performing its obligations under the Agreement, and any other purposes set out in the Agreement.

g. Privacy Laws means all New Zealand and Australian laws and regulations applicable to Personal Information, including the Privacy Act 2020 (NZ) and Privacy Act 1988 (Cth) (as applicable).

h. Service Provider means the counterparty to this Agreement.

i. Use in relation to Principal Data refers to any and all uses of and/or operations performed on Principal Data, including collecting, copying, creating, hosting, recording, organising, storing, adapting or altering, retrieving, using, analysing,

disclosing, making available, combining, blocking, anonymising, erasing and destroying Principal Data

2.2. CONSTRUCTION

a. In this Schedule, references to:

   i. "including" will be construed as "including, without limitation"; and

   ii. "related company" will have the meaning given to that term in the Companies Act 1993;

   iii. "related entity" will have the meaning given to that term in the Corporations Act 2001 (Cth).

b. If there is any conflict between the terms of this Schedule and the remaining terms of this Agreement, unless expressly and specifically stated otherwise, the terms of this Schedule prevail.

c. To the extent that any Principal Data is owned by a related company of Principal, the rights under this Schedule are intended to be for the benefit of that related company and enforceable by the related company for the purposes of Part 2, Subpart 1 (Contractual Privity) of the Contract and Commercial Law Act 2017 (NZ).

3. SERVICE PROVIDER OBLIGATIONS

3.1. USE OF PRINCIPAL DATA

The Service Provider undertakes that it will:

a. only use Principal Data strictly to the extent necessary for the Purpose(s);

b. only retain Principal Data for as long as reasonably necessary to achieve the Purpose(s) and in any event, ensure that all Principal Data is destroyed or returned to Principal (at Principal's election) at the end of the term of the Agreement or upon request from Principal at any time;

c. comply with all Privacy Laws in respect of all matters relating to Principal Data (even if the Service Provider is located outside New Zealand or Australia (as applicable));

d. not do or refrain from doing anything that would cause Principal to breach any Privacy Laws;

e. to the extent legally permitted, inform Principal of any third party (including subcontractors) to whom it discloses Principal Data (prior to such disclosure) and allow Principal reasonable opportunity to object to such disclosure (in such case, subject to its obligations to comply with the law the Service Provider must not disclose the relevant Principal Data);

f. inform Principal of the location that any Principal Data will be stored prior to storing the Principal Data and allow Principal reasonable opportunity to object to such location, in such case, the Service Provider will comply with any reasonable request made by Principal;

g. take all reasonable steps to ensure that it does not do or allow anything to be done which may identify or facilitate the identification of any individual whose identity has not been directly disclosed by Principal as part of Principal Data (including through any form of re-identification of anonymised information); and

h. not derive and/or use any anonymised or aggregated data from Principal Data (unless otherwise permitted by the Purpose(s) or agreed in writing with Principal).

3.2. SECURITY OBLIGATIONS

The Service Provider undertakes that it will:

a. provide appropriate training to personnel, which shall be provided no less than once per calendar year, with respect to the correct handling of Principal Data so as to ensure the Service Provider's compliance with its obligations under this Schedule;

b. ensure that Principal Data is protected by adequate security safeguards against a Data Breach (and, upon request from Principal at any time, provide Principal with written details of such security safeguards);

c. ensure that all Principal Data is segregated from the Service Provider's own data or that of the Service Provider's other customers;

d. if requested by Principal, restore Principal Data, if any Principal Data is lost, destroyed, corrupted or altered while in the Service Provider's or any subcontractor's possession or control;

e. not disclose any Principal Data to, or permit Principal Data to be Used by any third party, other than the sub-contractors expressly agreed to by Principal; and

f. not permit Principal Data to be transferred, outside New Zealand or Australia, without Principal's prior written consent. In the event that Principal provides consent for Personal Information to be transferred or stored offshore pursuant to this clause, the Service Provider must ensure that any offshore recipient of the Personal Information complies with all Privacy Laws in relation to that Personal Information. The Service Provider remains fully liable for any acts or omissions of the offshore recipient.

3.3. COMPLIANCE WITH SECURITY POLICIES

The Service Provider undertakes that it will perform its obligations under this Agreement that relate to Principal Data in such a way, and implement appropriate processes and technical measures, to ensure that it complies with:

a. Principal's policies that are applicable to Principal Data, notified to the Service Provider by Principal from time to time, including Principal's security policies and data breach response policies; and

b. any other terms relating to Principal Data set out in this Agreement or otherwise agreed in writing between the parties.

3.4. ASSISTANCE WITH AUDITS AND REQUESTS

The Service Provider undertakes that it will co-operate with, and provide assistance to, Principal in relation to:

a. the resolution of any request or complaint relating to Principal Data, including any such request or complaint under the laws or policies referred to in this Schedule; and

b. any audit that Principal may wish to undertake at any time in respect of Principal Data held by the Service Provider (including by providing access to the Service Provider's premises, personnel, processes and systems).

3.5. SERVICE PROVIDER MUST DELETE OR RETURN PRINCIPAL DATA ON REQUEST

The Service Provider undertakes that it will delete, or return, Principal Data to Principal:

a. in accordance with the retention periods set out in the Privacy Laws; or

b. at Principal's written direction, at any time during or after termination of this Agreement.

3.6. DATA BREACH

a. The Service Provider acknowledges that Principal relies on the Service Provider's compliance with this Schedule (including this section 3.6) to ensure that Principal complies with its obligations under the Privacy Laws, including in respect to any obligations regarding notification of data and privacy breaches.

b. The Service Provider undertakes that, if it is aware, or has reasonable grounds to suspect, that a Data Breach has occurred, to the extent permitted by law, the Service Provider will:

    i. notify Principal as soon as practicable, and in any event within 24 hours, after becoming aware that a Data Breach (or suspected Data Breach) has occurred (and keep Principal updated as additional information becomes available);

ii. promptly provide Principal with a detailed description of the Data Breach (or suspected Data Breach), including details of the type of data affected, number of affected individuals and a description of the likely consequences of the breach and any other information requested by Principal;

iii. provide all assistance and co-operation required by Principal in connection with the Data Breach (or suspected Data Breach) including in connection with Principal's obligations (if any) to notify the Data Breach to regulators or individuals (to the extent permitted by law, Principal will determine in its absolute discretion whether or not such notification is required); and

iv. keep the Data Breach (or suspected Data Breach) confidential or, if it notifies any third party of the Data Breach, not directly or indirectly identify Principal (unless it is required to do so by law, in which case the Service Provider will, to the extent permitted by law, consult with Principal prior to making any notification).

3.7. RESPONDING TO REGULATORS

Notwithstanding any other term of this Agreement, Principal may refer to the Service Provider and/or this Agreement in order to respond to and manage a Data Breach that involves the Service Provider.

3.8. SERVICE PROVIDER COMPLIANCE

The Service Provider must provide Principal with any information reasonably requested by Principal from time to time in order for Principal to confirm that the Service Provider is complying with this Schedule.

3.9. INDEMNITY

If the Service Provider breaches any of the obligations in this Schedule, the Service Provider will indemnify Principal against any liabilities, losses, costs, expenses, damages or claims suffered or incurred by Principal as a result of the breach.