MASTERBRAND

Corporate Policy – LG-001

Name: Enterprise Privacy Policy	**Version #: 1.0**
Owner: Chief Legal Officer	**Distribution: All MBC Associates**

I. Purpose

The purpose of this policy is to establish minimum global privacy and data protection standards for the processing of Personal Information (as defined below) and to implement basic concepts of privacy by default and privacy by design at MasterBrand, Inc., inclusive of all its majority owned subsidiaries or divisions ("MasterBrand" or "Company") (this "Policy"). This Policy also seeks to provide a single document that can direct associates and contractors to the various privacy procedures that MasterBrand has adopted to comply with Privacy and Data Security Laws (defined below) and that such associates and contractors must comply with

II. Scope

This Policy applies to all (1) Company associates, contractors, consultants, temporary workers, and other workers across the global enterprise ("Associates"), (2) Personal Information collected, maintained, transmitted, stored, retained, or otherwise used by the Company, regardless of the media on which that information is stored and whether relating to employees, customers, or any other person; and (3) business activities that process Personal Information.

III. Policy

a. Privacy Program – The Privacy Program will contain controls and procedures appropriate to Company's size and complexity, the nature and scope of Company's activities, and the sensitivity of the Personal Information, including:

i. The identification of reasonably foreseeable risks, both internal and external, that could result in a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise processed by or on behalf of Company and an assessment of the sufficiency of any safeguards in place to control these risks.

ii. The design and implementation of reasonable controls and procedures to address and mitigate such risks.

iii. Any other such reasonable controls, practices, or procedures as may be necessary to comply with the requirements of the Privacy and Data Security laws.

iv. Development of a mechanism for reasonable and appropriate testing or monitoring of the effectiveness of those controls and procedures that were set out as part of the Privacy Program.

b. Privacy Principles – Using, Handling, and Retaining Personal Information

i. Notice and Collection – Whenever the Company collects Personal Information for any purpose, it must inform the Data Subject of how it will use, process, disclose, protect, and retain that Personal Information. The Company may only collect Personal Information in compliance with applicable Company policies, and notices, and the Personal Information collected must be limited to that which is reasonably necessary to accomplish the Company's legitimate business purposes or as necessary to comply with law.

ii. Access, Use and Sharing of Personal Information – Associates may only access Personal Information to the extent such information relates to and is necessary to perform their job duties. Associates may not access Personal Information for any reason unrelated to their job duties. Associates may not use Personal Information in a way that is incompatible with the notice given to the Data Subject at the time the information was collected. If an Associate is unsure about whether a specific use or disclosure is appropriate, then the Associate should consult with their supervisor or a member of the Privacy Committee. Associates may only share Personal Information with another Associates if the recipient has a job-related need to know the information. Associates should only share and/or store Personal Information via encrypted methods. Please contact your division IT department for details on the type of encryption methods that can be used.

iii. Accuracy – Associates must collect, maintain, and use Personal Information that is accurate, complete, and relevant to the purposes for which it was collected.

iv. Security – Associates are responsible for protecting Personal Information. The Company has implemented several Cyber Security and Risk Policies that set forth technical, administrative, and physical safeguards for the protection of Personal Information. Associates must follow the security procedures set out in these Cyber Security and Risk Policies at all times. The Company's cyber security team can provide details on the Company's Cyber Security and Risk Policies. Associates must exercise particular care in protecting Sensitive Personal Information from loss, unauthorized access, and unauthorized disclosure.

v. Retention and Disposal – Associates should keep Personal Information only for the amount of time it is needed to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. Associates should follow the applicable records retention schedules and policies published from time-to-time by the Company's legal department and destroy any media containing Personal Information in accordance with the applicable records disposal policy.

vi. Reporting a Personal Information Security Incident – If an Associate knows or suspects that a Personal Information Security Incident has occurred, then they should not attempt to personally investigate the matter. Associates should immediately contact their supervisor or the Company's cyber security team at cybersecurity@masterbrand.com. Associates should preserve all evidence relating to the potential Personal Information Security Incident.

vii. Monitoring Compliance and Enforcement – The Privacy Committee is responsible for administering and overseeing implementation of this Policy and, as applicable, developing related operating procedures, processes, policies, notices, and guidelines. If an Associate is concerned that any provision of this Policy, or any related policy, operating procedure, process, or guideline designed to protect Personal Information, has been or is being violated, please contact privacy@masterbrand.com. The Company will conduct periodic reviews and audits to assess compliance with this Policy.

c. Privacy Committee

i. The Company will nominate relevant stakeholders from various Company departments, including but not limited to Legal, Human Resources, Internal Audit, Digital and Tech, and Cybersecurity, to participate in a committee that shall have the responsibilities as listed in this document and shall otherwise be accountable for the development, implementation, and maintenance of the Privacy Program.

ii. The Privacy Committee will implement and maintain policies and procedures that support this Policy and Company's Privacy Program. The Privacy Committee will also oversee the development, maintenance, and implementation of policies and procedures that will provide Data Subjects the ability to contact the Company about all issues related to processing of their Personal Information and to the exercise of their rights under the applicable privacy and data security laws.

iii. The Privacy Committee shall have the following responsibilities:

1. Lead and coordinate the drafting and implementation of the Privacy Program;
2. Maintain a working knowledge and understanding of legal and regulatory, cybersecurity, and privacy as set forth in the Privacy and Data Security Laws;
3. Monitor compliance with this Policy, the Privacy and Data Security Laws and other procedures of Company in relation to the protection of Personal Information;
4. As necessary and appropriate, provide advice and recommendations to Company's senior leadership, including the CEO and Board of Directors, on matters related to privacy and data security;
5. Support the Legal Department to cooperate with the regulatory authority or other government agencies;
6. Coordinate with the necessary Company departments to identify and assess reasonably foreseeable internal and external risks to privacy and security;
7. Collaborate with the appropriate departments and external partners (e.g., outside counsel) to develop policies, procedures, and controls to comply with the Privacy and Data Security Laws;
8. Work with the appropriate Company department to set reasonable minimum standards to protect the confidentiality, integrity, and availability of Personal Information processed by or on behalf of the Company;
9. Develop, implement, and revise as necessary, policies and / or procedures for managing third-party service providers, vendor and/or supplier in compliance with applicable Privacy and Data Security Laws; and
10. In collaboration with the appropriate internal and external partners, develop and implement training on Company's Privacy Program.

d. Vendor Management

i. The Company will comply with Privacy and Data Security Laws as they relate to the engagement of vendors who process Personal Information on behalf of Company or Personal Information received from Company. Please refer to Policy CS-010: Vendor Management.

ii. As required by Privacy and Data Security Laws, the Company shall ensure that vendors who will process Personal Information on behalf of Company: (a) provide sufficient guarantees to implement appropriate physical, technical, and organizational security measures in such a manner that such vendors' processing of Personal Information; (b)

provide means to assist MasterBrand in responding to Data Subject requests about Personal Information, such as understanding the content or removal of same; (c) will not collect, retain, use, or disclose Personal Information for any purpose other than as necessary for the specific purpose of performing the service to MasterBrand, including collecting, retaining, using, or disclosing the Personal Information for a commercial purpose other than providing the service to MasterBrand; and (d) will not sell the Personal Information in a context defined under applicable Privacy and Data Security laws as a "sale".

iii. The Company's engagement of vendors who will process the Personal Information on behalf of Company or Personal Information received from Company will be governed by a binding contract that includes appropriate security and privacy protection terms as required by Privacy and Data Security Laws.

e. Disposal and Destruction of Data – Company will retain records containing Personal Information to the extent necessary for business purposes or to comply with its obligations under applicable Privacy and Data Security Laws and destroy such records once those purposes have been accomplished in accordance with the requirements under applicable Privacy and Data Security Laws.

f. Privacy Training – The Privacy Committee shall establish programs for training Associates who process or have access to Personal Information which shall cover the relevant requirements of Privacy and Data Security Laws. Training may include, depending on the type of data and applicable law, proper handling of Personal Information to maintain confidentiality and integrity of the data and what to do in the event of a Personal Information Security Incident.

g. Individual Rights – The Company will implement and maintain procedures for receiving, logging, and responding to requests from Data Subjects. These procedures shall comply with the Privacy and Data Security Laws as they apply to Company. The Company will work with appropriate subject-matter experts to verify such compliance. Where the Company makes automated decisions based on processing Personal Information, including profiling, that may result in an adverse legal effect to Data Subjects, the Company will notify Data Subjects of this processing, provide individuals with an appeals process where they can challenge adverse decisions, as well as the ability not to be subject to such processing.

h. Incident Response

i. The Company has a documented Incident Response Policy (CS-009) with related procedures to handle Personal Information Security Incidents. This policy may be modified by Company at regular intervals.

ii. The Company will implement and follow procedures for responding to Personal Information Security Incidents in accordance with and as defined under applicable Privacy and Data Security Laws and its obligations therein.

iii. The procedures for responding to Personal Information Security Incidents shall include, where applicable, requirements for notice to the affected Data Subject(s) and regulatory authorities as required by Privacy and Data Security Laws. The Company will work with appropriate subject-matter experts to verify such compliance.

i. Privacy Impact Assessments

i. If the Company engages in processing of new Personal Information or changes the way it will process existing Personal Information in a manner that does or is likely to materially and negatively affect the rights of Data Subjects, then the Company will conduct a Privacy Impact Assessment ("PIA") to identify additional necessary safeguards will have to be conducted and determine whether the Company's documented standard privacy and security safeguards sufficiently address the privacy impact. If outstanding risks remain that the Company's standard safeguards cannot appropriately manage, remedial measures should be taken prior to the authorization of the processing activity at issue.

ii. Where the PIA indicates that the Personal Information of European Union ("EU") residents are involved and that there is a high risk to the EU residents' rights and freedoms, the Company will further conduct a Data Protection Impact Assessment ("DPIA") under appropriate supervision from Legal and/or outside legal counsel. The DPIA will help identify further necessary data protection measures and indicate whether prior consultation with the Company's regulatory authority would be appropriate.

j. Transfer of Data

i. For Personal Information subject to GDPR or where otherwise required by applicable Privacy and Data Security Laws, Company shall implement and maintain procedures to safeguard the transfer of Personal Information across national boundaries. These procedures shall comply with Privacy and Data Security Laws, and that compliance shall be verified by appropriate subject matter experts.

ii. For Personal Information transferred between corporate entities in different countries and subject to GDPR or where otherwise required by applicable Privacy and Data Security Laws, the Company shall draft and execute intra-company agreements between relevant corporate entities ensuring that transfers of Personal Information of data subjects shall be protected as required under Privacy and Data Security Laws.

k. Online Privacy Notice

i. Where required under Privacy and Data Security Laws, Company shall: (1) post on its public websites, domains, and mobile applications, a notice that explains how the Company processes Personal Information obtained through visitors' use of the sites, applications, and online services that are operated or controlled by Company; and (b) maintain this notice on its public websites and update as needed.

ii. When collecting Personal Information, as required under Privacy and Data Security Laws, the following information must be provided within the Privacy Notice:
    1. The contact details of the Company's privacy office;
    2. The purposes of the processing for which the Personal Information are intended as well as the legal basis for the processing;
    3. The recipients or categories of recipients of the Personal Information, if any;
    4. Where applicable, the fact that the Company intends to transfer Personal Information to third parties or transfer outside the country of origin, along with the purpose of the transfer.

IV. Definitions

a. Controller – Controller means the legal entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Information. In most cases, this will be the Company.

b. Data Subject – Any person whose Personal Information is processed by or on behalf of the Company. *See* Personal Information for examples.

c. Information Asset – A definable piece of information, regardless of format, which may be collected, developed, or otherwise processed by the Company. Information assets may include, but are not limited to, all forms and types of financial, business proprietary information, customer related information, strategies and processes, research and development, and personnel information.

d. Information Asset Owner – The Company associate responsible for the information assets within a Company business or department. The Information Asset Owner is knowledgeable about how the information asset is acquired, transmitted, stored, deleted, and otherwise processed.

e. Information Asset Custodian – The person who must maintain the protection of Information Assets according to the information classification associated with it and identified by the Information Asset Owner. Information Asset Custodians are responsible for the technical environment and / or underlying storage structure.

f. Personal Information – Any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household. This includes information that identifies, describes, or is capable of being associated with a known or identifiable individual's personal characteristics, communications and other works, surroundings and movements, and behaviors online and in the real world, such as data generated by an individual's personal use of a Company product or services. Personal Information also includes information that identifies or describes members of an individual's household, such as a postal address, home phone number, demographic information like number of members and household income levels, and information collected from shared use of the Company's products and services. Examples include: email addresses, names, phone numbers, postal addresses, IP addresses, location data, voice and video data of personal spaces, fingerprints and other biometric identifiers, and cookies and other information which may be used to identify a data subject or the subject's online browsing activity.

g. Personal Information Security Incident – Any act or omission, whether intentional or accidental, that compromises the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards the Company or a Third-Party Service Provider has put in place to protect Personal Information. The loss of or unauthorized access to, disclosure, or acquisition of Personal Information is a security incident.

h. Privacy and Data Security Laws – All relevant domestic and international privacy and data protection laws, current and future, governing privacy, data security, and Personal Information. Relevant laws include the California Civil Code Sec. 1798.100 resolution AB-375 (California Consumer Privacy Act ("CCPA")) for California residents, (EU) 2016/679 (General Data Protection Regulation ("GDPR")) for subjects of the European Economic Area and other similar laws and regulations in the U.S. and other jurisdictions where Company has physical operations or which govern Personal Information which Company processes (collectively, the "Privacy and Data Security Laws").

i. Privacy Committee – The committee appointed by the Company to lead and coordinate its Privacy Program. The Privacy Committee shall coordinate with other functions as necessary.

j. Privacy Program – A collection of policies and procedures, including this Policy, reasonably designed to (1) address privacy and data security risks related to Company's business operations, and (2) protect the privacy, confidentiality, integrity and availability of Personal Information processed by or on behalf of the Company.

k. Processing – Any operations which are performed on Personal Information or on sets of Personal Information, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, or through transmission.

l. Processor – In relation to Personal Information, a Processor is any person or entity (other - than an associate or other personnel of the Data Controller) who processes the data on behalf of a Data Controller and strictly for the purposes of providing the contracted-for services to the Data Controller. Processors, including where MasterBrand acts as a Processor, do not: (a) collect, retain, use, or disclose Personal Information for any purpose other than as necessary for the specific purpose of performing the service to the Data Controller, including collecting, retaining, using, or disclosing the Personal Information for a commercial purpose other than providing the service; or (b) sell the Personal Information.

m. Sensitive Personal Information – Specific Personal Information, where its unauthorized access, processing or disclosure may result in increased risk of harm to a Data Subject. Examples include: GDPR Special Categories (listed below), data affecting the data subject's rights and freedoms in a negative way, financial data, location data, or social security numbers. If applicable Privacy and Data Security Laws further define Sensitive Personal Information or additional requirements on entities who process such data, then those laws would also apply. Certain types of sensitive personal information are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as "special categories" of personal data. The special categories are:

i. Personal data revealing racial or ethnic origin.
ii. Political opinions.
iii. Religious or philosophical beliefs.
iv. Trade union membership.
v. Genetic data and biometric data processed for the purpose of uniquely identifying a natural person.
vi. Data concerning health.
vii. Data concerning a natural person's sex life or sexual orientation.

Processing of these special categories is prohibited, except in limited circumstances set out in Article 9 of the GDPR. For the purposes of this document Personal Information and / or Sensitive Personal Information will be collectively referred to as "Personal Information."

V. Related Policies

Other Company policies also apply to the collection, use, storage, protection, and handling of Personal Information and may be relevant to implementing this Policy, including the Cyber Security and Risk Policies. You should familiarize yourself with these policies, including:

- Global Information Security Policy Framework
- Acceptable Use Policy
- Access Management Policy

March 16, 2023