CYBER SECURITY POLICY STATEMENT

MasterBrand Cyber Security

MasterBrand, Inc. ("MasterBrand") is committed to protecting the confidentiality and integrity of our data, as well as the data of our employees and customers, at all times. The mission of MasterBrand's cyber security program is to protect the assets used to create products, generate revenue, and service customers while meeting compliance with all applicable laws and industry frameworks. MasterBrand's cyber security program consists of three key pillars: cyber defense, governance and compliance, and risk management. Each of these pillars consists of controls and processes that are derived from the NIST Cyber Security Framework, or NIST CSF.

Managing cyber security risk and maintaining a secure, reliable, and functional corporate network and data systems is among the highest priorities at MasterBrand. As a result, MasterBrand has implemented practices, procedures, and management mechanisms to help ensure that we achieve a robust cyber security environment.

Governance

Cyber security matters fall under the purview of the Company's dedicated VP, Cyber Security and Risk, a seasoned executive with experience in cyber security and certified as both a Certified Information Security Services Professional (CISSP) and Certified Ethical Hacker (CEH).

This individual reports to both the Board and the Audit Committee at least once a year. The Committee reviews and discusses with Company management key process and risk indicators, progress on plans to address keys risks, and any material changes in threat landscapes or risk posture which could negatively affect company.

Risk Management

MasterBrand's cyber defense practices prioritize protection against cyber threats, and the Company has operationalized a standard incident response process. MasterBrand performs periodic cybersecurity assessments, including with the assistance of external third parties, to identify, assess, and prioritize potential risks that could affect the Company's information and data assets and infrastructure. If any such risks are identified, MasterBrand addresses them.

Our governance and compliance practice focuses on policy taxonomy and ensuring compliance with those policies as well as applicable laws and regulations, including those linked to data privacy.

MasterBrand has implemented a number of measures to enhance the security and resiliency of our network and information/data systems. These measures include, but are not limited to: (i) user access control management; (ii) intrusion detection and prevention systems; (iii) information security continuity measures, including redundant systems and information backups; (iv) network segmentation; (v) encryption of critical information and data; (vi) event logging; (vii) implementation of an application patching and update cadence; and (viii) incident response planning.

Training and Awareness

MasterBrand employees are a critical part of our defense against potential cyber security incident exposure. All MasterBrand employees and contractors have a responsibility and a role to play by complying with the Company's cyber security operational practices and reporting any potential cyber security incidents or exposures to the MasterBrand cyber security team.

To ensure that employees can play their part in protecting the Company's networks and data from cyber security incident exposure, all MasterBrand employees receive cyber security training in the form of online modules on an annual basis, routine simulations, and newsletters.