



VISANT HOLDING CORP.

VISANT CORPORATION

AND

SUBSIDIARIES

CODE OF BUSINESS CONDUCT AND ETHICS

Introduction/General Statement

The following Code of Business Conduct and Ethics (“Code”) sets forth the guiding principles for the conduct of the business of Visant Holding Corp. (“Visant”) and its subsidiaries (collectively, the “Company” or as the context dictates, a subsidiary of Visant) in accordance with applicable law, our internal policies and procedures and high ethical standards to ensure that the Company’s core values of honesty, fair dealing, ethical business practice, and full disclosure are followed by all.

Compliance with the Code

UNDERSTANDING THE CODE

The Company takes this Code very seriously. All of us must take personal responsibility for conducting ourselves in a way that reflects positively on our business and advances the principles set forth in this Code. All employees must follow the ethical standards set forth in this Code and are obligated to report, in a timely fashion, any possible violations of our ethical standards that they may witness. Reporting in good faith possible ethical violations by others will not subject an employee to reprisal. In fact, retaliation or punishment for reporting suspected unethical or illegal conduct by another employee as provided in this Code or for coming forward to alert the Company of any questionable situation is against the law.

This Code applies to all of our directors, officers, employees and independent sales representatives. We refer to all persons covered by this Code as “Company employees” or simply “employees”. We also refer to our Chief Executive Officer, our principal financial officer, our principal accounting officer and our corporate controller as our “principal financial officers”.

It is the responsibility of employees to read carefully and understand this Code. This Code is not intended to be a comprehensive rulebook and cannot address every situation that you may face. If an employee is concerned about an ethical situation or is not sure whether specific conduct meets the Company’s standards of conduct, employees are responsible for asking their supervisors, managers or other appropriate personnel any questions that they may feel are necessary to understand the Company’s expectations of them.

VIOLATIONS OF THE CODE

Employees who fail to comply with these policies, including supervisors who fail to detect or report wrongdoing, may be subject to disciplinary action, up to and including termination. The determination of discipline will be based upon the facts and circumstances of each particular situation. An employee accused of violating the Code will be given the opportunity to present his or her version of the events at issue prior to the Company’s determination of appropriate discipline. The following are examples of conduct that may result in discipline:

- actions that violate a Company policy
- requesting others to violate a Company policy
- failure to raise promptly a known or suspected violation of a Company policy
- failure to cooperate in a Company investigation of a possible violation of a Company policy
- retaliation against another employee for reporting a possible violation or concern

It is important to understand that violation of certain of these policies may subject the Company and the individual employee involved to civil liability and damages, regulatory sanction and/or

criminal prosecution. The Company is responsible for satisfying the regulatory reporting, investigative and other obligations that may follow the identification of a violation.

REPORTING VIOLATIONS; CONFIDENTIALITY

The Company has established procedures throughout the Code for employees to use for getting help with a potential issue or reporting a problem. When you believe you or another employee may have violated the Code or an applicable law, rule or regulation, it is your responsibility to immediately report the violation to your supervisor or to a representative of the local Human Resources department. If your supervisor or local HR representative cannot answer your question or you do not feel comfortable contacting your supervisor or local HR representative, please contact the Company's General Counsel either in writing sent to the attention of General Counsel, Visant Corporation, One Byram Brook Place, Suite 202, Armonk, New York 10504, or by telephone at 914-595-8211. Similarly, if you are a supervisor, manager or HR representative and you have received information from an employee concerning activity that he or she believes may violate the Code or that you believe may violate the Code, you should report the matter to the General Counsel or your local Legal Department representative promptly.

Additionally, the Company has established a Hotline that is available 24 hours a day, 7 days a week at 1-877-VISANT4 (1-877-847-2684) to report a possible violation of this Code. You may remain anonymous and will not be required to reveal your identity in calls to the Hotline, although providing your identity may assist the Company in addressing your concern. You will be able to call back to follow-up on the status of your report. Calls made to this number are forwarded to the Company's General Counsel for investigation and resolution (as warranted, with the involvement of the appropriate level of management). Matters regarding accounting, internal accounting controls or auditing matters are forwarded to the Internal Audit Department and the Audit Committee of the Board of Directors for investigation.

All reports and inquiries will be handled confidentially to the greatest extent possible under the circumstances. As mentioned above, no person will be subject to retaliation or punishment for reporting suspected unethical or illegal conduct by another employee as provided in this Code or for coming forward to alert the Company of any questionable situation.

CERTIFICATE OF COMPLIANCE

On an annual basis, the Company will ask its principal financial officers to certify that they are "aware of and are in compliance with the Company's policies on ethical behavior." Similarly, other employees will be asked on a regular basis to certify to their familiarity and compliance with the Code.

In addition, all new employees will be given a copy of the Code (or referred to an electronic copy) and will be informed that compliance with this Code is a condition of their employment.

WAIVER OF COMPLIANCE

In certain limited situations, the Company may waive application of the Code to employees. Waivers of this Code for employees may be made only by an executive officer of the Company. Any waiver of this Code for our directors, executive officers or other principal financial officers may be made only by our Board of Directors or the appropriate committee of our Board of Directors and will be disclosed to the public as required by law or stock exchange rule.

Conflicts of Interest

A “conflict of interest” may occur when an employee’s private interest interferes, or reasonably appears to interfere, with the interests of the Company as a whole. A conflict situation can arise when an employee takes actions or has interests that may make it difficult to perform his or her company work objectively and effectively. Conflicts of interest also arise when an employee, or a member of his or her family, receives improper personal benefits as a result of his or her position in the Company. Each employee should avoid any private interest that influences his or her ability to act in the interest of the Company or makes it difficult to perform his or her work objectively and effectively.

Identifying potential conflicts of interest may not always be clear-cut. The following situations are examples of possible conflicts of interest:

- Employees’ primary employment obligation is to the Company. Any outside activity, such as a second job or self-employment, must be kept completely separate from their activities with the Company. Employees may not use Company customers, suppliers, time, name, influence, assets, facilities, materials or the services of other employees for outside activities unless specifically authorized by the Company.
- No employee should be employed by, serve as a director of, or provide any services to a company that is a material customer, supplier or competitor of the Company.
- No employee should obtain any material (as to him or her) personal benefits or favors because of his or her position with the Company. Please see “**Gifts and Gratuities; Entertainment**” below for additional guidelines in this area.
- No employee should have a significant financial interest (ownership or otherwise) in any company that is a material customer, supplier or competitor of the Company. A “significant financial interest” means (i) ownership of greater than 1% of the equity of a material customer, supplier or competitor or (ii) an investment in a material customer, supplier or competitor that represents more than 5% of the total assets of the employee.
- No employee should obtain loans or guarantees of personal obligations from, or enter into any other personal financial transaction with, any company that is a material customer, supplier or competitor of the Company. This guideline does not prohibit arms-length transactions with banks, brokerage firms or other financial institutions.
- No employee should serve on a board of directors or trustees or on a committee of any entity (whether profit or not-for-profit) whose interests reasonably would be expected to conflict with those of the Company.
- The actions of family members outside the workplace may also give rise to the conflicts of interest described above because they may influence an employee’s objectivity in making decisions on behalf of the Company. For purposes of this Code, “family members” include your spouse or life-partner, brothers, sisters and

parents, in-laws and children whether such relationships are by blood or adoption.

Disclosure of Conflicts of Interest

The Company requires that employees disclose any situations or transactions that reasonably would be expected to give rise to a conflict of interest. Any such situation or transaction should be avoided unless specifically approved. If you suspect that you have a conflict of interest, or something that others could reasonably perceive as a conflict of interest, you must report it to your supervisor or the Legal Department. Your supervisor (in coordination with the Legal Department) will work with you to determine whether you have a conflict of interest and, if so, how best to address it. Although conflicts of interest are not automatically prohibited, they are not desirable and may only be waived as described in “**Waiver of Compliance**” above.

Corporate Opportunities

As an employee of the Company, you have an obligation to advance the Company’s interests when the opportunity to do so arises. If you discover or are presented with a business opportunity through the use of corporate property, information or because of your position with the Company, you should first present the business opportunity to the Company before pursuing (or directing a third party to pursue) the opportunity in your individual capacity. No employee may use corporate property, information or his or her position with the Company for personal gain or to compete with the Company.

You should disclose to your supervisor the terms and conditions of each business opportunity covered by this Code that you wish to pursue. Your supervisor will contact the General Counsel and the appropriate management personnel to determine whether the Company wishes to pursue the business opportunity. If the Company waives its right to pursue the business opportunity, you may pursue the business opportunity on the same terms and conditions as originally proposed and consistent with the other ethical guidelines set forth in this Code.

Gifts and Gratuities; Entertainment

Any payment made to a third party must be made only for identifiable services that were performed by the third party for the Company or one of its customers. In addition, the payment must be reasonable in relation to the services performed.

Employees are not permitted to give, offer or promise payments or gifts with the intent to influence (or which may reasonably appear to influence) a third party or to place such party under an obligation to the donor. It is your responsibility to use good judgment in this area. As a general rule, you may give or receive gifts or entertainment to or from customers or suppliers only if the gift or entertainment would not be viewed as an inducement to or reward for any particular business decision. All gifts and entertainment expenses should be properly accounted for on expense reports. Gifts and entertainment should not compromise, or reasonably appear to compromise, your ability or the third party’s ability to make objective and fair business decisions. Any gift or entertainment should be consistent with good customary business practices and not excessive in value. No gift should be given or accepted in violation of applicable law, and no gift or entertainment should be solicited. Additional restrictions are imposed on dealings with foreign, federal, state or local government officials. Gifts and entertainment may not be offered to or exchanged under any circumstances with any employee of the U.S., state or local governments. There are also other public, as well as private, institutions that have established their own internal

rules regarding the acceptance of gifts or entertainment. Employees should become familiar with any such restrictions affecting those with whom they deal.

There are some cases where refusal of a valuable gift would be offensive to the person offering it. This is particularly true when employees are guests in another country, and the gift is something from that country offered as part of a public occasion. In these cases, the employee to whom the gift was offered may accept the gift on behalf of the Company, report it to management and turn it over to the Company.

The Company, as a responsible corporate citizen, can make donations of money or products to worthy causes, including fundraising campaigns conducted by its customers. To remain an appropriate donation, the contribution should not be connected to any specific customer purchases or purchasing commitments.

Customer requests for donations of significant sums of money should be forwarded to a senior-level manager in your organization. Employees are not permitted to make a donation at a customer's request and then seek reimbursement from the Company as a business expense. All corporate donations must be approved and paid by the Company. Please discuss with your supervisor or the Legal Department any gift or proposed gift which you are not certain is appropriate.

Protection and Use of Company Assets

Employees should protect the Company's assets and ensure their efficient use for legitimate business purposes only. Theft, carelessness and waste have a direct impact on the Company's profitability. The use of Company funds or assets for any unlawful or improper purpose is prohibited.

To ensure the protection and proper use of the Company's assets, each employee should:

- Exercise reasonable care to prevent theft, damage or misuse of Company property.
- Report the actual or suspected theft, damage or misuse of Company property to a supervisor.
- Use the Company's telephone system, other electronic communication services, written materials and other property primarily for business-related purposes.
- Safeguard all electronic programs, data, communications and written materials from inadvertent access by others.
- Use Company property only for legitimate business purposes, as authorized in connection with your job responsibilities.

Employees should be aware that Company property includes all data and communications transmitted or received to or by, or contained in, the Company's electronic or telephonic systems. Company property also includes all written communications. Employees and other users of this property should have no expectation of privacy with respect to these communications and data. To the extent permitted by law, the Company has the ability, and reserves the right, to monitor all

electronic and telephonic communication. These communications may also be subject to disclosure to law enforcement or government officials.

Participation in unlawful activities or possession of illegal items or substances by an employee, whether on Company property or business or not, jeopardizes the employee's employment with the Company.

Confidential Information

Employees have access to a variety of confidential information while employed at the Company. Confidential information includes all non-public information that might be of use to competitors, or, if disclosed, harmful to the Company or its customers. Employees have a duty to safeguard all confidential information of the Company or third parties with which the Company conducts business, except when disclosure is authorized or legally mandated. An employee's obligation to protect confidential information continues after he or she leaves the Company. Unauthorized disclosure of confidential information could cause competitive harm to the Company or its customers and could result in legal liability to you and the Company. Any questions or concerns regarding whether disclosure of Company information is legally mandated should be promptly referred to the Legal Department.

Confidential information includes, but is not limited to:

- Computer programs, data, formulas, software and compositions
- Customer, employee and supplier information
- Financial data
- Inventions
- Manufacturing processes and techniques
- Marketing and sales programs
- Compensation information
- New product designs
- Possible acquisition or divestiture activity
- Pricing information and cost data
- Regulatory approval strategies
- Research and development information
- Services techniques and protocols
- Trade secrets and know-how
- Strategic business plans

Except as specifically authorized or legally mandated, employees, consultants, agents and representatives are expected to maintain the confidentiality of information entrusted to them by the Company or its customers and shall not disclose or use, either during or subsequent to their employment by or the term of any other relationship with the Company, any such information they receive or develop during the course of Company employment or any such other relationship with the Company, which is non-public or considered proprietary by the Company or its customers. Confidential information may be disclosed within the Company only on a need-to-know basis (and subject to other restrictions as may apply to the specific information). Employees should not attempt to obtain confidential information that does not relate to their employment duties and responsibilities.

Employees, consultants, agents and representatives may not discuss confidential matters in the presence or within hearing range of unauthorized persons, such as in elevators (even on Company property), restaurants, taxis, airplanes or other publicly accessible areas. Care should be used in the use of cellular telephones or other means of communication that are not secure.

In instances where it is appropriate for business reasons to disclose Company confidential information to third parties, the Legal Department must be contacted before the disclosure for preparation of an appropriate agreement that includes the necessary safeguards.

Furthermore, obtaining confidential information from a third party without adequate legal safeguards is improper and may expose the Company to legal risks. Accordingly, no employee, consultant, agent or representative may accept such information without the advice of the Legal Department and until an agreement in writing has been reached with the offeror. After such information is obtained, its confidentiality must be protected as provided in the agreement.

No employee, consultant, agent or representative may disclose or use any confidential information gained while providing services to the Company for personal profit or to the advantage of the employee or any other person.

Computer and Other Electronic Resources and Computer Security

The Company's computer resources are Company assets. Computer resources include, but are not limited to, all of the Company's processing hardware, software, networks and networking applications, and associated documentation, and include voicemail and email systems. The Company expects all employees utilizing our computer and other electronic resources to observe the highest standard of professionalism at all times. This includes respecting and maintaining the integrity and security of all Company computer and communication systems, and utilizing those systems for the furtherance of Company business. It also includes respecting the values of the Company, and each individual within it, by creating and sending only appropriate business-related messages. To this end, the following policies and principles apply:

- Employees are responsible for ensuring the integrity and confidentiality of their unique user identification codes and passwords. Any suspected breach must be reported to appropriate management immediately.
- Employees are not permitted to access a computer without authorization or to exceed authorized access with the intent of securing information which they are not authorized to access.
- Employees are expected to log out of systems that do not support an automated log out process when leaving them unattended.
- Employees are not permitted to alter, damage or destroy information without authorization.
- Employees may not obstruct the authorized use of a computer or information.
- Employees are not permitted to use the Company's computer resources for personal gain.
- Computer programs developed by employees using the Company's computer resources and developed within the scope of the employee's employment or other Company relationship are the Company's property. All rights to and use of such property are reserved by the Company.
- Unless prohibited by applicable law in the jurisdiction, the Company reserves the right to monitor without further notice its computer resources.
- Employees' use of electronic mail systems, the Internet, or other electronic facilities shall be limited primarily to business related communications, and employees must adhere to applicable supervisory and regulatory requirements when utilizing such systems as part of

