CODE OF CONDUCT

Version: October 14, 2021

Our Corporate Creed

Always Tell the Truth

We do not lie, cheat, or steal or engage in unethical, illegal, or immoral behavior. We will willingly lose a sale or customer in order to comply with the law and our consciences.

Always Produce Safe, High-Quality Products in Safe and Secure Facilities

We are absolutely and passionately committed to producing safe and quality products made in accordance with the highest manufacturing standards. Our workers and facilities must meet or exceed all environmental, health, and safety standards. We work diligently to ensure the physical security of all of our employees and facilities.

Always be Professional

We always dress and behave professionally as a sign of respect for each other, our Company, and our business partners.

These principles are non-negotiable. They are the foundation of everything we do.

In everything we do, we aspire to will the good of each other and our world.

Our Commitment To Ethical Standards

General Policy and Procedures for Business Conduct

Sensient Technologies Corporation and each of its subsidiaries (the "Company") has a proud history of good corporate citizenship and compliance with the law. The Company will always conduct its business as a good corporate citizen and will comply with all laws and regulations applicable to us. This policy applies to all full-time or part-time employees of the Company, as well as all directors, including members of the Scientific Advisory Committee, and officers ("Employees"). It must be strictly observed.

Employees are prohibited from engaging in conduct that violates any applicable international, federal, state, or local law, rule, or regulation. Such conduct is outside an Employee's scope of employment with the Company. All Employees are expected to maintain high standards of business and personal ethics and honesty while performing their work, consistent with the professional image of the Company.

The Code of Conduct (the "Code") sets forth the standards and procedures to be followed by Employees to ensure that Company business is conducted in a lawful and ethical manner. The Code is intended to be a guide for Employees. It does not address all of the laws we encounter in the conduct of our business. The Code is not an employment contract, and the Company may modify or repeal the provisions of the Code or adopt a new Code at any time it deems appropriate, with or without notice.

All Employees are responsible for understanding the Code and for acting in accordance with it. To this end, Employees are encouraged to seek guidance regarding the application or interpretation of the Code from the Corporate Legal Department. Questions regarding any law, rule, or regulation which may govern business conduct, but which is not specifically addressed in the Code, also should be directed to the Corporate Legal Department.

The Company will exercise due diligence in attempting to prevent and detect unethical or unlawful conduct by its Employees.

In addition, Employees are required to question possible misconduct and resolve any misconduct issues through the procedures outlined in the Code. Employees are required to promptly report violations of law or of the Code in the manner provided herein. Internal reporting is also explicitly encouraged (though not required) by the SEC's whistleblower bounty rules.

All Employees are required to cooperate fully in any investigation of a potential violation.

The Company will conduct periodic training on the provisions of the Code. The Code and the periodic training are designed to give Employees the tools they need to help the Company comply with applicable laws and to operate consistently with high standards of business and personal ethics. This will avoid actions that could cause harm to the Company and will communicate to our shareholders and the community that we manage our business conduct as diligently as we manage our business operations.

Reporting Possible Violations ("Whistleblower Procedures")

If any Employee believes the Code has been violated, he or she must promptly report the matter to the General Counsel or Director, Internal Audit. The report must be truthful. Reports may be verbal or in writing, and may be made on a confidential or anonymous basis using the compliance concerns form on the Sensient intranet at https://sensus.sensient-tech.net/legal/Lists/Legal%20concerns%20form/NewForm.aspx?source=http://sp2013prod.sensient-tech.net/legal/. When requesting confidential or anonymous treatment, Employee should indicate that request prominently. In all cases, Employees should include sufficient information about the complaint or concern so that it can be properly investigated.

Except in the case of a confidential or anonymous submission, the Company encourages the person submitting the complaint or concern to provide his or her name, address, and phone number, as well as his or her relationship with the Company and its auditors. This will help the Company to focus its investigation of the matter, and also to report back concerning its resolution of the complaint or concern, when appropriate.

Confidentiality will be maintained to the fullest extent possible, consistent with the need to conduct an adequate review and investigation.

Every Employee must cooperate in the investigation of suspected violations.

All reports of violations will be promptly investigated and remedied as appropriate under the direction of the General Counsel. The General Counsel will enlist the support of Internal Audit and Human Resources as appropriate. All investigations will be conducted consistent with applicable national laws. The General Counsel will report the results of all investigations of alleged violations to the Audit Committee of the Board of Directors on a quarterly basis. The Chief Executive Officer will provide anonymized reports to all employees regarding violations of the Code on a regular basis.

Reports of violations relating to accounting, auditing, internal controls, or compliance matters ("Compliance Matters") will be promptly forwarded to the Chairman of the Audit Committee and will be reviewed and investigated under Audit Committee direction and oversight by such persons as the Audit Committee determines to be appropriate, which

may include the General Counsel, Director, Internal Audit, and outside legal, accounting, or other advisors. Prompt and appropriate corrective action will be taken when and as warranted in the judgment of the Audit Committee. The Audit Committee will retain as part of its records all reports of complaints or concerns regarding Compliance Matters and their treatment. The General Counsel will assist the Audit Committee by maintaining files regarding all reports, tracking their receipt, investigation, and resolution, and will prepare a periodic summary report thereof for the Audit Committee.

As appropriate or required, the violation will be timely reported to the proper government authorities.

The General Counsel and the Corporate Legal Department will conduct periodic reviews of reporting trends, and, if appropriate, implement measures necessary to prevent recurrence of such violations.

The Company will not discharge, demote, suspend, threaten, harass, or in any manner discriminate against any employee in the terms and conditions of employment based upon any lawful actions of such employee with respect to good faith reporting of complaints or concerns regarding Compliance Matters. It is a crime in the United States and elsewhere to retaliate against, harass, or dismiss a person for providing truthful information to a company's internal compliance and reporting system, a government official, or a regulatory agency. Any supervisor intimidating or imposing sanctions on an Employee for reporting a matter will be disciplined, up to and including termination. In the United States, Employees who allege that they have been retaliated against for providing information to a federal agency, Congress, or a person with supervisory authority over the Employee about suspected fraud may file a complaint with the Department of Labor or in federal court.

The United States Securities and Exchange Commission (SEC) has established rules that can potentially pay rewards to Employees or others who report significant misconduct either internally to the Company or to appropriate enforcement authorities. Those rules expressly encourage (but do not require) that reports be made internally to the Company by providing that voluntary participation in a company's internal compliance and reporting system is a factor that can increase the amount of an award, while interfering with a company's internal compliance and reporting can decrease the amount of an award. The rules also provide that if a company receives a report to its internal compliance and reporting system and, after investigating the matter, reports it to the SEC, the reporting Employee will get credit -- and a potentially greater reward -- for any additional or more specific information generated by the company in its investigation. Employees should also understand that it is a crime in the United States to willfully make a materially false statement to a government agency.

Employees are also advised that the Code does not prohibit an Employee from providing information to a Federal regulatory or law enforcement agency, any member of Congress, or any committee of Congress, in connection with conduct that the Employee reasonably believes constitutes a violation of a criminal statute (including antifraud statutes) or any

SEC rule or regulation.

Additionally, nothing in the Code limits an Employee's right to file any charge or complaint of employment discrimination with administrative agencies such as the United States Equal Employment Opportunity Commission and nothing in the Code will be construed to prevent an Employee from communicating with any government agency regarding matters that are within the agency's jurisdiction.

Furthermore, an Employee cannot be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that is (1) made in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and solely for the purpose of reporting or investigating a suspected violation of law; or (2) in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.

Finally, an Employee who files a lawsuit for retaliation by the Company for reporting a suspected violation of law may disclose the trade secret to his or her attorney and use the trade secret information in the court proceeding, provided that the Employee (1) files any document containing a trade secret under seal; and (2) does not disclose a trade secret, except pursuant to a court order.

Consequence of Violations

Any Employee who violates the Company's Code will be subject to disciplinary action, up to and including termination.

The response will depend upon a number of factors, including whether the improper behavior involved illegal conduct. Disciplinary action may include, but is not limited to, reprimands and warnings, probation, suspension, demotion, reassignment, reduction in salary, or immediate termination. All Employees should be aware that certain actions and omissions prohibited by the Code might be crimes that could lead to individual criminal prosecution and, upon conviction, to fines and imprisonment.

Supervisors and managers of the disciplined Employee may also be subject to disciplinary action for their failure to properly oversee Employee conduct or for retaliation against Employees who report violations.

The Code will be enforced on a uniform basis for all Employees, without regard to their position within the Company.

Accounting Matters

This section sets forth specific the standards and procedures to be followed by our Chief Executive Officer, President, Chief Financial Officer, principal accounting officer, controller, and all other persons performing similar functions anywhere in the world for the Company (the "Senior Financial Officers") to ensure that Company business is

conducted in a lawful and ethical manner. All Employees are responsible for following the Company's internal controls.

Disclosure Controls and Procedures

U.S. federal and state securities laws impose continuing disclosure requirements on the Company, and require the Company to regularly file certain reports (the "Reports") with the Securities and Exchange Commission and the New York Stock Exchange and then to disseminate these Reports to its shareholders. Such Reports must comply with all applicable legal and exchange requirements and may not contain statements which, at the time made, are false or misleading with respect to a material fact, omit any material fact necessary to prevent a statement from being false or misleading, or omit any material fact necessary to correct any earlier statement which has become false and misleading.

A set of disclosure controls and procedures has been adopted by the Company in connection with these continuing disclosure requirements. The Controller's Department maintains a checklist of disclosure controls and procedures for external quarterly financial reporting. All Senior Financial Officers must inform themselves and strictly adhere to such controls and procedures in the preparation of Reports. In addition, all Senior Financial Officers and all representatives who assist the Company in such Reports and communications will ensure that such Reports and communications (i) are full, fair, timely, factual, accurate, and understandable, and (ii) meet all legal requirements. This policy applies to all public disclosure of material information about the Company, including written disclosures, oral statements, visual presentations, press conferences, and media calls.

Internal Controls

Internal Controls are policies and procedures designed to safeguard the Company and its assets and to ensure accurate financial record keeping. The Company's internal accounting control policies and procedures are published in the Accounting and Finance Manual, which is available on the Company's intranet at http://sensus.sensient-tech.net/functions/Finance/Documents%20Public/Accounting%20and%20Finance%20Manual.pdf. It is the responsibility of business unit, Group, and Corporate management, including Senior Financial Officers, to establish a proper control environment and procedures. Local management must take measures and actions necessary to ensure that all Employees understand and comply with the procedures for appropriate internal controls. In addition, it is the responsibility of the business unit, Group, and Corporate Controllers, to approve, on a monthly basis, the control procedures and activities summarized in the Monthly Financial Statement Certification.

An effective system of internal controls will include physical controls over assets and procedures designed to ensure that all entries in the Company's books and records are accurate and complete. All Company assets, liabilities, revenues, and expenses will be recorded in the official books of record. Compliance with generally accepted accounting principles and established internal controls are required at all times.

The Internal Audit Department will monitor compliance with established internal controls at each location, review the adequacy, appropriateness, and efficiency of the control

procedures, and make recommendations to management for improvements in these procedures. Any questions regarding the system of internal controls should be addressed to the Director, Internal Audit.

If any Senior Financial Officer or Employee becomes aware of a violation of an internal control, or receives direction to violate an internal control, he or she must immediately report such violation or direction to the Chief Executive Officer and General Counsel.

Accounting, Auditing, and Other Matters

The Company is committed to achieving compliance with all applicable securities laws and regulations, accounting standards, accounting controls, and audit practices. This includes both internal audit and accounting functions as well as those functions performed by and in conjunction with the Company's outside auditors. Senior Financial Officers will not circumvent compliance with these accounting and auditing laws, standards, controls, and practices, nor assist any third party in circumvention. If any Senior Financial Officer believes such compliance has been violated, the matter should be promptly reported to the Audit Committee. The Company's Audit Committee will oversee treatment of employee concerns in this area. *See Reporting Possible Violations*. Senior Financial Officers should take measures and actions necessary to help ensure that all employees understand and comply with these accounting and auditing laws, standards, controls, and practices.

Antitrust Laws

***See* Antitrust Compliance Manual (Appendix)**

Antiboycott Laws

The U.S. Export Administration Act and the 1976 Tax Reform Act contain provisions commonly known as the Antiboycott Laws. The Antiboycott Laws were enacted in response to the Arab boycott of Israel and are designed to prevent U.S. firms and their foreign affiliates from taking part in boycotts that the U.S. government does not sanction. Under these laws, U.S. citizens and firms (including foreign affiliates) are prohibited from taking or agreeing to take certain actions in support of unauthorized boycotts. These actions include:

- refusing to do business with the subject of the boycott, including using, or agreeing to use, blacklists;
- discrimination against a person on the basis of race, religion, or national origin or furnishing such information about a person;
- furnishing information about business relationships with or in Israel or with blacklisted companies; and
- implementing a letter of credit containing certain prohibited conditions.

Violations of these provisions are punishable by criminal and civil penalties and administrative sanctions, including suspending or revoking the authority to export and

denial of tax benefits for boycott-related agreements. The Antiboycott Laws have strict reporting requirements, and any activity or questions that relate to these matters must be reported to the Corporate Legal Department immediately.

Authority to Act on Behalf of the Company

No Employee may commit the Company or any of its subsidiaries to any contract, agreement, or other obligation unless such Employee is authorized to do so. Prior to signing any documentation on behalf of the Company or any of its subsidiaries, Employees are required to confirm that they have authority to bind the Company or its applicable subsidiary under the Code, legally, and as a matter of internal policy. Please contact the Corporate Legal Department for any questions related to signing authority for the Company or any of its subsidiaries.

All contracts, agreements, or other obligations (i) between the Company and a customer, (ii) involving individual or aggregate amounts in excess of $10,000 USD, or (iii) with a duration of longer than one year, must be approved by the Corporate Legal Department before signing.

Bribery

***See* Anti-Bribery Policy (Appendix)**

Communicating Extraordinary Matters to the CEO

To ensure that the Company's Chief Executive Officer has all information necessary to discharge his responsibilities, Company Employees with responsibility for any proposed commercial transaction that is not in the ordinary course of the Company's business must communicate promptly and fully with the Company's Chief Executive Officer regarding such matters. Examples of such extraordinary matters include, but are not limited to, those involving product safety, significant capital expenditures, long-term contractual commitments, or exposure to significant potential liability.

Communications with Analysts and the Media

The Company must speak with a unified voice in all dealings with the press and other media, and in all dealings with securities analysts, other investors, and investment professionals. As a result, except as otherwise designated by the Company's Chief Executive Officer, the Senior Vice President and Chief Financial Officer, or the Vice President and Treasurer are the only authorized contacts for discussions with investors, investment professionals, and securities analysts concerning our company. Except as otherwise designated by the Company's Chief Executive Officer, other Employees are prohibited from communicating with any investor, investment professional, or securities analyst.

Except as otherwise designated by the Company's Chief Executive Officer, the Senior Vice President and Chief Financial Officer, or the Vice President and Treasurer are the only authorized contacts for interviews with the media concerning our Company. This prohibition also does not preclude employees protected by the National Labor Relations Act from exercising Section 7 rights that they may have to communicate about working conditions, or in any way limit the rights of those employees to participate in any investigation by the National Labor Relations Board.

Company Property

All Employees must protect the Company's property and assets and ensure their efficient use. Any Employee who intentionally steals or misappropriates, or intentionally or negligently damages or wastes, Company property will be subject to discipline, up to and including termination.

Any suspected incident of fraud or theft must be reported immediately as described in Reporting Violations section above.

Confidentiality

***See* Company Confidential Information Policy (Appendix)**

Conflicts of Interest

Except with the prior knowledge and consent of the Company, conflicts between an Employee's personal or private interests and those of the Company are not permitted.

A potential conflict of interest exists when an Employee has any position with, or a substantial interest (financial or otherwise) in, any other business or matter that would conflict or might reasonably appear to conflict with the proper performance of the Employee's job responsibilities or the Employee's independent and objective judgment with respect to transactions between the Company and the other business.

A conflict of interest can only be determined after reviewing the particular circumstances in the context of the Employee's activities with the Company. The following list serves as a guide to the types of activities that might create a conflict of interest, but is not exclusive.

- **Interest in entities transacting business with the Company.** Employees may not have a financial interest in a supplier, competitor, or customer of the Company. This includes, but is not limited to, ownership by an Employee or any member of his or her family of more than 5% of the stock either directly or indirectly in any outside concern that does business with the Company, except where such interest consists of securities of a publicly-owned corporation and such securities are traded on the open

market (unless such investments are of such a size as to have influence or control over the corporation). Employees will not have an interest in or perform any services for a supplier or customer of the Company except for owning a small minority interest in securities of a publicly owned company.

- **Gifts.** Employees and their family members may not accept from any individual or company providing goods or services to the Company any gift of more than token value, loans (other than from established banking or financial institutions), or hospitality or entertainment which could influence the Employee's independent judgment. This does not include gifts of nominal value, entertainment, meals, or social invitations which are customary and proper under the circumstances; support the achievement of a valid business purpose; are consistent with the high standards of business ethics required in the conduct of all Company business activities and relationships; and do not place the Employee under an obligation of any kind.
- **Loans**. The Company will not extend, maintain, or arrange for any personal loan to or for any director or officer unless (1) there are extraordinary circumstances; (2) the loan is approved by the Board of Directors; and (3) all required disclosures are made under SEC and NYSE rules and regulations.
- **Use of Company assets.** Employees are responsible for ensuring that corporate assets are used only for valid corporate purposes. Company assets include our equipment, inventory, corporate funds, and office supplies. They also include our concepts, business strategies and plans, confidential information, trade secrets, financial data, intellectual property rights, and other information about our business. These assets may not be improperly used to provide personal gain for Employees or others.
- **Company opportunity.** Employees owe a duty to the Company to advance its legitimate interests when the opportunity to do so arises. Employees are prohibited from (i) taking personal advantage of opportunities that are discovered through the use of corporate property, information, and position, (ii) using corporate property, information, or position for personal gain, and (iii) competing with the Company. Employees will not buy or sell for themselves or their family any security or property interest which they know the Company may be considering buying or selling until the Company has publicly announced its decision regarding the transaction and has concluded its interest in the subject.
- **Transactions.** Employees will not compete with the Company directly or indirectly in the purchase or sale of property or products without full disclosure to the Corporate Legal Department.
- **Conflicting roles.** Employees cannot represent the Company in any transaction in which the Employee or any family member has a substantial interest.
- **Employment outside the Company.** Employees will not accept employment outside the Company that adversely affects the manner in which an Employee performs duties or fulfills responsibilities to the Company.
- **Service on other boards.** No Employee may accept an appointment as a member of the board of directors or as an officer of any other Company, trade association, charitable, or educational organization, without prior written approval by the Corporate Legal Department (***See*** **Request for Approval to Serve on Other Boards** form in the Appendix). Board memberships for charitable organizations, educational

institutions, or similar organizations are encouraged, as long as no potential or actual conflict of interest exists.

- **Participation in testing or standards setting organizations.** Employees may participate in such organizations only after disclosure to and the approval of the Corporate Legal Department.
- **Communication of conflicts.** All potential and actual conflicts of interest or material transactions or relationships that reasonably could be expected to give rise to such a conflict or the appearance of such a conflict must be communicated as provided under **Reporting Possible Violations** above. If you have any doubt about whether a conflict of interest exists after consulting this provision of the Code, please contact the Corporate Legal Department so that they can help make that determination.

Cybersecurity

The Board of Directors oversees the Company's Cybersecurity Program, including the following elements:

- On an annual basis, the Board of Directors must define high risk cybersecurity areas for the Company and implement comprehensive programs to address these risks. High risk areas will be reviewed and revised as needed.

- Management must report at least twice annually to the Board of Directors on cybersecurity progress and effectiveness.

- The Company will maintain an executive level steering committee (including the CEO, CFO, Group Presidents, General Counsel, and Director of IT) to meet monthly and provide oversight of cybersecurity.

- The Company will conduct mandatory annual employee training programs, quarterly cyber executive incident response simulations, and regular cyber penetration testing.

- The Company will continue to make investments as required in its technical capabilities in all areas of security.

If any Employee becomes aware of an actual or a suspected cybersecurity risk or incident, including vulnerabilities and breaches, the matter must be promptly reported to the Director of IT and the General Counsel. *See* **Reporting Possible Violations**.

Director Confidentiality Policy

Pursuant to their fiduciary duties of loyalty and care, directors are required to protect and hold confidential all non-public information obtained due to their directorship position. Unless required by law to disclose such information, directors may not disclose Confidential Information (as defined below) unless they first obtain the express permission of the Board.

Accordingly:

- no director may use Confidential Information for his or her own personal benefit or to benefit persons or entities outside the Company, including other shareholders;
- no director may discuss Confidential Information, specific potential or actual Company business operations or transactions with anyone outside of the Company, including other shareholders;
- no director may discuss Confidential Information in public settings or other settings where inadvertent disclosure may occur;
- no director may disclose Confidential Information outside the Company, including to other shareholders, either during or after his or her service as a director of the Company;
- upon a director's departure from the Company, the director must return all originals and copies of documents or materials containing Confidential Information; and
- if a director discloses Confidential Information or learns that someone else has, whether intentionally or inadvertently, the director must immediately report the disclosure to the Corporate Legal Department.

For purposes of this subsection, "Confidential Information" means all non-public information entrusted to or obtained by a director by reason of his or her position as a director of the Company. It includes, but is not limited to, non-public information that might be of use to competitors or harmful to the Company or its customers if disclosed, such as:

- non-public information covered by SEC Regulation FD;
- non-public information about the Company's financial condition, prospects or plans, leases, trade secrets, compensation and benefit information, marketing and sales programs, and research and development information, as well as information relating to mergers and acquisitions, stock splits, and divestitures;
- non-public information concerning possible transactions with other companies or information that the Company is under an obligation to maintain as confidential about the Company's customers, suppliers, or joint venture partners;
- non-public information about an actual or a suspected cybersecurity risk or incident, including vulnerabilities and breaches, related to the Company or its customers, suppliers, or joint venture partners; and
- non-public information about discussions and deliberations relating to business issues and decisions between and among Employees, executive officers, and directors.

Document Retention

The law requires the Company to maintain certain types of corporate records, usually for specified periods of time or when litigation is pending or threatened. Failure to retain

those records for those minimum periods could subject the Company to penalties and fines, cause the loss of rights, obstruct justice, place the Company in contempt of court, or seriously disadvantage us in litigation.

From time to time the Company establishes document retention or destruction policies in order to ensure legal compliance. All Employees must fully comply with our published Corporate Record Retention Policy. If an Employee believes, or the Corporate Legal Department informs you, that Company records are relevant to pending or potential litigation or any government inspection or other regulatory action, then all Employees must preserve those records until the Company determines that the records are no longer needed. This exception supersedes any previously or subsequently established document destruction policies for those records. If an Employee believes that this exception may apply, or has any questions regarding the applicability of this exception, please contact the Corporate Legal Department.

Electronic Communications

Employees have access to the Company's electronic communication system, which includes computers, telephones (including Company-issued cell phones or smart phones), voice mail, facsimile machines, e-mail, and the Internet when accessed through a Company computer. The purpose of this system is to enhance job performance on day-to-day assignments and to facilitate effective business communications. Employees' actions and communications on the Company's electronic communication system may be attributed to the Company, which could be held responsible for Employees' actions. Therefore, this policy outlines the proper uses of the electronic communication system.

- **Ownership.** The Company's electronic communication system is Company property. All messages, information, and data sent and received by the electronic communication system are Company property. Incidental and occasional personal use of the electronic communication system is allowed, but such use will be subject to this policy and any resulting messages and data are the property of the Company. This personal use is allowed when it does not interfere with an Employee's work performance, interfere with any other Employee's work performance, unduly impact the operation of the electronic communication system or violate any other provision of this or any other Company policy. Company-related text messages should not be sent other than through Company-issued cell or smart phones and the Company's cell phone provider.
- **No privacy.** Even though Employees have unique user log-in identification codes and passwords to access the electronic communication system, Employees have no privacy in the use of any part of the electronic communication system or in any documents, messages, or information created on, with, or transmitted over the system. The Company has access to the system and maintains the right to access and monitor, consistent with the law, all documents, messages, and information created on, with, or transmitted over the system, including e-mail and Internet usage, without notice to Employees. Employees are deemed to consent to that access and review, provided that the Company will access stored text messages only when it has a reasonable

suspicion that the messages relate to a violation of Company policy or any applicable law and then only as reasonably required for that purpose and in accordance with all applicable national laws. All such documents, messages, and information can be reviewed by the Company and law enforcement.

- **Monitoring.** The Company reserves the right to monitor and access the electronic communication system and all documents, messages, or information created on, with, or transmitted over the system. These Company rights will be exercised strictly in accordance with applicable law, the Company's business purposes (which include ensuring the appropriate use of the system), and in cooperation with requests from law enforcement. The Company also reserves the right to disclose such documents, messages, or information when consistent with the Company's business purposes and with requests from law enforcement.
- **No offensive use.** Employees accessing the electronic communication system are identifiable as Employees of the Company. Employees therefore must recognize that they may be viewed as representatives of the Company when they access the system and they must conduct themselves appropriately. Employees may not use the electronic communication system in an offensive, harassing, illegal, or defamatory manner. This prohibition does not preclude employees protected by the National Labor Relations Act from exercising Section 7 rights that they may have to communicate about working conditions or in any way limit the rights of those employees to participate in any investigation by the National Labor Relations Board. The Company prohibits the use of the electronic communication system to send or receive offensive or improper messages such as sexually explicit or pornographic messages, images, cartoons, or jokes; unwelcome propositions, requests for dates, or love letters; profanity, obscenity, slander, or libel; ethnic, religious, sexual, racial, or other slurs; messages containing political beliefs or commentary; or any other message that could be construed as harassment or disparagement of others.
- **Pornography, Sexually Explicit, and Other Offensive Material.** Viewing, downloading, or possessing any pornographic, sexually explicit, or other offensive material on the Company's electronic communication system is prohibited.
- **Confidential information, solicitation, and illegal activities.** Employees may not improperly disclose confidential Company information and materials in any manner, including via the electronic communication system. Nor may Employees use the system to solicit for commercial activities, religious, or political causes, outside organizations, or other non-company related matters. Employees also may not use the electronic communication system for illegal activities or purposes.
- **Copyrights, trademarks, and patents.** Employees must not violate copyrights, trademarks, or patents. An Employee may not copy, download, or use any image, text, video, audio material, software, or other copyright-protected, trademark-protected, or patented data without appropriate authorization. This restriction applies to copying copyrighted, trademarked, or patented materials from someone else, the local area networks, or the Internet.
- **Software.** The Company expressly prohibits the unauthorized use or duplication of copyrighted software. The Company will provide legally acquired software to meet the legitimate Company software needs in a timely fashion and in sufficient quantities for all Employees. The Company will comply with all license or purchase terms regulating the use of any software acquired or used by Employees. Employees may

not engage in or tolerate the making or using of unauthorized software copies under any circumstances. Employees may not remove, obscure, or alter any copyright or proprietary notices associated with any Company software or related software packaging materials. The Company will enforce reasonable internal controls to prevent the making or using of unauthorized software copies, including reasonable measures to verify compliance with these standards and appropriate disciplinary measures for violation of these standards.

- **Electronic communication system and data.** Only Company authorized software and related encryption software tools may be used in connection with the Company electronic communication system and all related data. Employees may not use non-Company licensed or owned software or encryption software tools. The Company prohibits Employees from using any software or encryption software tools to access Company data located on the Company electronic communication system, unless authorized to do so. Employees may not disassemble, decompile, reverse engineer, or tamper with any software or encryption software tools to prevent the Company from accessing or recovering any and all encrypted information.
- **Right to search.** The Company reserves the right to inspect and search all computers, electronic devices, and components of the electronic communication system found on Company property without notice to ensure that Employees are complying with this and other Company policies. Such inspections and searches will be conducted in accordance with all applicable laws.
- **Off-duty conduct.** An Employee who maintains a web site must not use Company equipment or working time to maintain the web site. Any off-duty online conduct by an Employee must not interfere with the Employee's ability to perform his or her job effectively, and must not adversely affect productivity in the workplace.
- **Personal digital assistant devices and smart phones.** All of the foregoing requirements also apply when an Employee uses any Company cell or smart phone or any other personal device that connects with the Company's electronic communication system. Additional concerns (such as preventing the accidental introduction of computer viruses and retaining e-mails and other documents whenever litigation is pending or threatened) also arise. Accordingly, Employees are not allowed to use personal digital assistants like a Blackberry, iPod, flash or thumb drive, smart phones, pocket PC, MP3, and the like to access the Company electronic communication system unless the device is provided or approved by the Company and is used for Company-authorized purposes.

Environmental, Health, and Safety Policy

We are committed to the principles of sound environmental management, protection of Employee health and safety, and responsible use of energy and natural resources. We view these principles as important aspects of the Company's economic health and core values. We expect each Employee to actively participate in and contribute to this Corporate philosophy.

Each Employee and each Company-owned or operated facility will comply with all applicable local, state, and federal environmental, health, and safety ("EHS") laws and

regulations. All Company facilities will be operated in a manner to protect the health of our workers through the adoption of appropriate work practices and to avoid harm to the environment, prevent pollution, and reduce waste generation through the adoption of appropriate environmental management systems.

All Employees will be appropriately trained and are expected and required to perform their jobs in a safe manner. The Company strictly prohibits: (a) reporting for work or working while under the influence of intoxicating beverages or controlled substances or any other form of impairment; (b) the possession, transmittal, or receipt of intoxicating beverages or the unlawful manufacture, distribution, dispensing, receipt, possession, or use of controlled substances or drug paraphernalia while on the job, while on the Company premises (including lunch or other break periods), while on Company business, or while operating or riding in a Company vehicle; and (c) the use of alcohol or illegal sale, transmittal, receipt, possession, or use of controlled substances off premises that adversely affects work performance, safety, or the reputation of the Company. Applicants for employment must pass a pre-employment drug test. All employment offers are contingent upon passing a drug test.

Corporate EHS Department

The Corporate EHS Department has the responsibility and authority to establish policies, standards, and initiatives related to Company activities which may impact the environment or Employee health and safety. This Department oversees, monitors, and measures environmental, health, and safety performance at every facility and has full access to all Company facilities, records, property, and personnel relating to EHS matters. The Department promotes awareness of environmental and health and safety issues and consults with internal and external stakeholders. In conjunction with, and at the direction of, the Corporate Legal Department, the EHS Department is responsible for providing definitive interpretation of laws, rules, and regulations related to EHS compliance, for hiring outside consultants to assist with such determinations, and for conducting internal EHS compliance audits at designated Company facilities.

Group Presidents, General Managers, and Plant/Facility Managers

Group Presidents and General Managers are responsible for ensuring compliance with applicable federal, state, and local EHS laws and regulations and for implementing Corporate EHS policies and programs at their respective facilities. Plant/Facility Managers are responsible for developing and implementing procedures to ensure that each activity, facility, source, or condition attains and remains in compliance with Corporate policies and programs and applicable EHS laws and regulations; Plant/Facility Managers are also responsible for general emergency preparedness, hazard identification, and risk assessment. Various duties associated with this responsibility may, at the discretion of the Plant/Facility Manager, be delegated to other facility personnel. However, the Plant/Facility Manager remains responsible for overall day-to-day facility compliance.

EHS Audits

Periodic third-party audits are conducted at Company facilities to determine the state of facility compliance with applicable EHS laws and regulations. Corrective actions are

implemented as necessary. All EHS audits will be conducted as authorized by the Corporate EHS Department at the direction of the Corporate Legal Department or the Audit Committee of the Board of Directors.

Consequences of Non-Compliance

The consequences of non-compliance with EHS laws and regulations can be severe:

- The Company can be subject to significant civil and criminal penalties and prison time for individuals;
- Employees can be held personally liable for fines and penalties;
- Harm could result to the environment and surrounding communities;
- Facilities may be subject to shutdown; and
- Adverse publicity could lead to a negative impact on the Company's ability to do business.

Violations of Company EHS policies or EHS laws and regulations are violations of the Code and will subject any Employee who violates such policies or laws and regulations to disciplinary action provided for by the Code. Given the potential grave consequences of unsafe behavior on the safety and well-being of our workforce, any Employee who violates a Company EHS policy or otherwise works in a manner that unreasonably compromises the safety of that Employee or any other Employee is subject to disciplinary action, up to and including termination.

Equal Employment Opportunity

The Company values the dignity of each employee as a unique person with an individual skill set and perspective. We categorically reject individuals and ideologies that seek to sow hate, discord, and division based upon an individual's personal characteristics. We have been and always will be one Sensient at all times and in all places, united by our common humanity and our common dedication to the Sensient Corporate Creed.

Sensient provides equal employment opportunities to all people based upon individual merit alone. Sensient will comply with all national, state, and local Equal Employment Opportunity laws, orders, and regulations in the conduct of its activities.

The Company will not discriminate based upon race, religion, color, sex (which includes pregnancy, orientation, identification, expression, and all other legally protected characteristics), age, national origin, disability, veteran or military status, political beliefs, or any other characteristic now or subsequently protected by applicable law (collectively, "protected classes").

The Company will administer all policies, benefits, and programs, including but not limited to those relating to interviewing and selection, compensation, promotion, transfer, layoff, recall, and training, on a nondiscriminatory basis and in accordance with applicable law and the Corporate Creed.

Failure to provide equal employment opportunities, including those listed above, to a person because of that person's status in a protected class is a violation of this policy and of the law and will not be tolerated or condoned by the Company. Upon proof of a violation of this Section, the offending employee will be summarily terminated with no payment beyond that which a government mandates must be made.

The Vice President, Human Resources and his or her staff are responsible for developing and administering procedures designed to ensure compliance with this policy.

Export Controls

The United States has a number of laws and regulations that govern (and sometimes outright prohibit) sales and purchases of certain products by U.S. companies and their foreign subsidiaries to certain countries.

It is the Company's policy to comply with all applicable U.S. and non-U.S. export control statutes and regulations as summarized in the *Sensient Technologies Corporation Export Compliance Policy*. All Employees must fully comply with the *Sensient Technologies Corporation Export Compliance Policy* and violations will be punishable as provided in the Code.

It is critical to consult with the Corporate Legal Department before even discussing a possible sale or purchase of any product that may be subject to U.S. and/or non-U.S. export controls.

Facility Visits

***See* Sensient Physical Security Policy**

Fair Dealing

The U.S.'s Federal Trade Commission Act prohibits "unfair methods of competition" and "unfair or deceptive acts or practices." While this Act overlaps somewhat with the other antitrust statutes, it goes beyond them by including all "unfair" acts, such as business conduct that deceives or misleads the consuming public. No Employee may engage in unfair methods of competition or unfair or deceptive acts or practices.

Every Employee must endeavor to deal fairly with the Company's customers, suppliers, competitors, and other Employees. No Employee should take unfair advantage of any person through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair-dealing practice.

Foreign Corrupt Practices Act and Other Anti-Corruption Laws

***See* Anti-Bribery Policy (Appendix)**

Fraternization Policy

The Company prohibits any supervisor or manager from dating or carrying on a romantic relationship with any subordinate. In addition, Company officers (elected and appointed), the highest ranking manager ("Senior Manager") at each of the Company's international business operations and locations, and human resources directors and managers are prohibited from dating or carrying on a romantic relationship with any Employee or other person who regularly works for a temporary agency or as a contractor at Company facilities. Such relationships can be disruptive to the work environment, create a conflict or the appearance of a conflict of interest, and could lead to charges of favoritism, discrimination, and claims of sexual harassment. While the Company has no desire to interfere with the private lives of its Employees or their off-duty conduct, where such conduct may affect the work environment, the Company will take appropriate action to protect its interests.

The terms "dating" and "romantic relationship," as used in this policy, include but are not limited to: casual dating, serious dating, casual sexual involvement, cohabitation, and any other conduct or behavior normally associated with romantic or sexual relationships. The policy is not intended to discourage friendship between supervisory and non-supervisory personnel. Any Employee engaged in a romantic or dating relationship with another Employee is required to notify the Employee's Human Resources Manager or Director, or the Corporate Vice President, Human Resources. Employees in violation of this policy may be subject to discipline, up to and including termination of employment.

Governmental Inspections, Inquiries, and Investigations

The Company will cooperate as required by law with authorized representatives of all governmental authorities conducting an inspection, inquiry, or investigation of the Company or other companies.

Governmental inspections of Company facilities are to be handled in accordance with the Company's *Governmental Inspections Manual*, which contains procedures to be followed during the course of all governmental inspections, including procedures for internal notification and reporting of inspections.

Any Employee who receives notice, whether verbal or written, of a governmental inquiry or investigation (e.g., request for information concerning compliance status of the Company or a Company facility, notice of noncompliance, notice of violation, etc.) must immediately communicate such information to his or her responsible Plant, Facility, or General Manager. It is imperative that all governmental inquiries and investigations be

properly communicated to management and coordinated at all levels within the Company and that all inquiries by the authorities be handled in an orderly manner. Since governmental inquiries and investigations are generally conducted under the authority of law, the responsible Plant, Facility, or General Manager must immediately notify the Corporate Legal Department of the inquiry or investigation. The Corporate Legal Department will participate in any inquiry or investigation in which the Company becomes or might become involved.

All Employees who receive requests, whether oral or written, for access to Company files, records, or information of any nature during the course of a government investigation or where such request is pursuant to a criminal or civil subpoena must immediately refer such requests to the Corporate Legal Department. No Company information may be furnished to an outside governmental investigator in response to such a request without consultation with the Corporate Legal Department.

Employees are advised that criminal penalties, including imprisonment, may be imposed upon any person who submits false or misleading information to, or otherwise obstructs, the government in connection with a governmental investigation. This may include statements made to the government which deny any wrongdoing on the part of the Company, even if such wrongdoing occurred without the Employees' knowledge. Proper legal supervision of any response, verbal or written, made to governmental authorities is essential.

None of the provisions in this section are intended to diminish the protections afforded to Employees against retaliation in connection with the provision of information to specified entities or persons, as described in **Reporting Possible Violations**.

Harassment

The Company does not tolerate workplace violence. Accordingly, any Employee who is determined to have assaulted, battered, or threatened any person, regardless where occurring will be terminated. Assault includes using, brandishing, or threatening to use any weapon in the workplace or against any Employee regardless of where occurring. Battery includes any intentional physical touching that is harmful or offensive regardless of whether injury results. A threat means a statement of present or future intent to assault, batter, or otherwise physically harm someone. ***See*** **Sensient Physical Security Policy**.

The Company prohibits intimidation and harassment based on race, color, national origin, religion, sex (which includes pregnancy, orientation, identification, expression, and all other legally protected characteristics), age, disability, genetic condition, veteran or military status, political beliefs, or any other characteristic protected now or subsequently by any applicable local, state, or national law.

Intimidation and harassment include behavior that interferes with an Employee's performance by creating a difficult, intimidating, hostile, or offensive working environment, and can arise from a broad range of physical or verbal behavior (by

Employees or by non-Employees such as customers or outside contractors). Conduct in violation of this policy can include, but is not limited to, physical or mental abuse; racial, ethnic, or religious insults or slurs; unwelcome sexual advances or touching; sexual comments, jokes, stories, or innuendos; requests for sexual favors used as a condition of employment or affecting any personnel decision such as hiring, promotion, compensation, or termination; display of sexually explicit or otherwise offensive posters, calendars, or materials; sending sexually explicit or suggestive electronic communications; making sexual gestures with hands or body movements; asking personal questions about another Employee's sexual life; and repeatedly asking out an Employee who has stated that he or she is not interested. Any Employee who is found to have engaged in such conduct is subject to immediate discipline, up to and including termination.

These activities are offensive and are inappropriate in the workplace. This is a serious issue not just for the Company but also for each individual. An Employee or supervisor may be held individually liable as a harasser and subject to the same penalties which may be imposed upon employers under state or federal law. This policy against harassment applies throughout our work environment, whether in the office, at work assignments outside the office, at office-sponsored social functions, or otherwise.

In addition, no Employee of the Company should have to tolerate harassment from any customer, vendor, or other person doing business with the Company or others with whom we come in contact in the course of our work-related duties. While the Company's ability to influence the conduct of customers, vendors, or others who engage in such behavior may be limited, we are committed to taking appropriate action, to the extent practical, to protect and assist our Employees. If an Employee becomes aware of such behavior, he or she must **immediately** report it to the General Counsel.

Harassment or similar unacceptable activities that could become a condition of employment or a basis for personnel decisions, or that create a hostile, intimidating, or offensive environment are specifically prohibited. Any Employee who engages in such harassment or retaliates against another Employee because the Employee made a good faith report of harassment, or participated in an investigation of a claim of harassment, is subject to immediate discipline, up to and including termination.

If any Employee believes that he or she has witnessed or has been the subject of prohibited harassment or retaliation:

- If comfortable doing so the Employee should first speak to the person who has engaged in the inappropriate behavior about his or her conduct.
- If not comfortable speaking to the person who has engaged inappropriate behavior, or if the inappropriate behavior does not stop, or if the Employee is not satisfied with the result of the discussion with the offender, the Employee must report the inappropriate conduct as provided for in the Code, as stated under *Reporting Possible Violations*, immediately.
- Any report of sexual harassment received by any supervisor or manager must be immediately reported to the General Counsel.

It is important that the Employee immediately inform the Company about the inappropriate conduct, because the Company cannot do anything to remedy the problem if it does not know that it exists. Any such reports will be investigated promptly and be kept confidential within the bounds of our investigation and the law. All Employees are expected to cooperate fully in any investigation concerning harassment.

This prohibition does not preclude U.S. Employees protected by the National Labor Relations Act from exercising Section 7 rights that they may have to communicate about working conditions or in any way limit the rights of those employees to participate in any investigation by the National Labor Relations Board.

Insider Trading

"Insider trading" refers to two types of conduct, one that is legal and one that is illegal. The legal form of insider trading occurs in certain circumstances when Company executive officers or directors buy or sell stock in the Company. These transactions must be publicly reported through filings with the Securities and Exchange Commission (the "SEC"). Even though this type of insider trading may be legal, it is ***essential*** that any officer or director buying or selling Company stock do so only in strict compliance with Company policy as laid out in the Appendix to the Code.

But in addition to this legal form of insider trading, there exists an illegal form: trading in a stock when in possession of material, nonpublic information. This type of illegal trading includes both instances where any Company director, officer, or other Employee trades stock for his or her own benefit as well as instances where the director, officer, or other Employee provides material, nonpublic information to another person who trades – even if the person providing the information does not know about the trade -- based on that information. This latter scenario is known as "tipping." It is a violation of Company policy and federal and state law to engage in illegal insider trading. This applies not only to Company stock, but also securities of our customers, suppliers, and even competitors and peer companies.

What constitutes material, nonpublic information is a complex legal question that depends on the specific facts of a particular situation. However, it may be generally stated that information is material if an ordinary investor would most likely take that information into account when deciding whether to buy, sell, or hold securities and that information is nonpublic if it has not been disseminated to the general public. All Employees may be in possession of material non-public information from time to time and must adhere to the restrictions of U.S securities law.

For example, information about the Company's earnings, a merger or acquisition in which the Company is involved, the launch of a new product by the Company, the entering into or loss of a major Company contract, or an actual or a suspected cybersecurity risk or incident would all be considered material. So, too, would information about management changes or information related to Company stock, such as

a change in the Company's dividend or a stock split. Whenever this sort of information has not been released to the general public, it will constitute material, nonpublic information. These examples are not exhaustive. Any questions about what information can be discussed should be directed to the General Counsel or Treasurer.

Illegal insider trading can lead to serious penalties for both the individual who trades on the basis of the material, nonpublic information and for companies that fail to safeguard adequately against the misuse of such information by enacting a system of monitoring and control of directors, officers, and other employees.

Because of the severe penalties associated with illegal insider trading, the Company has established the following policies, in addition to the director confidentiality policy described above:

- Employees must maintain the confidentiality of material, nonpublic information and not disclose it to any third party, except where such disclosure is part of an official Company statement distributed to the general public (e.g., a press release).
- Directors and officers of the Company may engage in transactions in Company securities only during the Company's trading "window period," which is described in the Appendix to the Code.
- No director, officer, or other Employee may engage in any transaction involving Company stock or other Company securities at any time when he or she is in possession of material, nonpublic information, or at any time before 24 hours has passed following public disclosure of such material information.

Any questions about Company policies with respect to insider trading should be directed to the Corporate Legal Department. In addition, the Appendix to the Code contains more information about insider trading, including Company policies relating to insider trading.

Inventions

Unless applicable national law is to the contrary, all inventions are the exclusive property of the Company. *Inventions* are marketable ideas, discoveries, developments, improvements, innovations, and know-how, whether patentable or not, which are conceived, reduced to practice, or made by Employees. Employees will promptly disclose all inventions in writing to the General Counsel. This includes inventions created while working for Sensient Technologies Corporation either solely or in concert with others (whether or not the others are Employees of the Company). These inventions must be disclosed whether or not they are:

- made or conceived during working hours;
- relate in any manner to the existing or contemplated business or research activities of the Company;
- are suggested by or result from the Employee's work at the Company; or
- result from the use of the Company's time, materials, or facilities.

Employees must assign to the Company their entire right, title, and interest to all inventions that are the property of the Company under the provisions above and to all unpatented inventions that they own, except those specifically described in a statement which has been separately executed by the Employee. At the Company's request and expense, the Employee will execute specific assignments to any such invention and take such further action as may be considered necessary by the Company at any time during or subsequent to the period of their employment to obtain and defend letters patent in any and all countries and to vest title in such inventions in the Company or its assigns.

Any invention disclosed by an Employee to a third person or described in a patent application filed by them or on their behalf within six months following the termination of their employment with the Company will be presumed to have been conceived, reduced to practice or made by them during their employment with the Company. However, this does not apply if the former Employee can prove the invention was conceived, reduced to practice, and made by them following the termination of employment with the Company and was not related to its business or research activities; was not suggested by or did not result from the Employee's work at the Company; or did not result from using the Company's time, materials, or facilities.

Certain Employees may be required to sign separate confidentiality agreements due to the type of work they perform or their position with the Company (e.g., Employees who work in research and development or who are hired to create inventions).

In countries that have national laws that may render any of the above obligations unenforceable, Employees will assist the Company with establishing ownership of the inventions in compliance with the national laws.

Legal and Ethical Compliance

The Company and its Employees are subject to a complex web of U.S. and national laws. The Company requires that all Employees comply with all of the laws, rules, and regulations of the United States and other countries, and of the states, counties, and cities where we do business, including all laws related to wages, working hours, working conditions, freedom of association, and all other labor and employment laws. Employees may not circumvent the application of these laws. Neither the Company nor its Employees may assist any third party in violating the laws of any country.

Global human rights are fundamental to the operations of Sensient's business. Human rights are rights, freedoms, and standards of treatment regarded as belonging to all persons. Sensient respects and supports internationally recognized human rights and is committed to high standards of ethics, honesty, and integrity and demonstrating respect and dignity for one another and those with whom we do business.
We also seek to work with suppliers that employ practices that meet or exceed all applicable laws. These requirements and expectations for ourselves and our suppliers include, without limitation, the matters described below. In the event local standards on a matter do not exist or do not meet these ethical standards, the Company and our

suppliers must nevertheless establish employment practices and will apply U.S. standards where appropriate while complying with local law. Compliance with the law and observing our ethical obligations are absolutely essential conditions for fulfilling our duties to each other, our customers, and society as a whole. We reserve the right to inspect the operations and records of our suppliers to establish compliance with these standards.

Employees with knowledge or information concerning any illegal or unethical behavior by the Company or our suppliers should report it immediately to the General Counsel. ***See*** **Reporting Possible Violations**. Our minimum requirements and expectations include but are not limited to:

- **No forced labor.** The use of forced labor of any kind is strictly prohibited, including prison labor, non-rescindable contracts, or labor obtained through threats of punishment, deposits of bonds, or other constraints. All employment with the Company must be strictly voluntary. The Company does not tolerate involuntary labor of any kind, and will not do business with any person or entity that is involved with or facilitates human trafficking. The use of physical acts to punish or coerce workers, the use of psychological coercion, or any other form of physical or non-physical abuse is prohibited.

- **No child labor.** The Company prohibits the exploitation of children and use of illegal child labor. Work by children under the age of 15 years (or any higher age established by applicable law) is strictly prohibited. Human Resources will ensure that all employees are legally eligible for employment and meet the applicable minimum legal age. Human Resources will maintain, in accordance with applicable laws, verifiable documentation of each employee's date of birth, or some legitimate means of confirming each employee's age.

- **No harassment or abuse.** The Company strictly prohibits harassment and abuse by all Employees. ***See*** **Harassment**. We also expect our suppliers to treat their employees with respect and dignity, and without harassment or abuse of any kind.

- **Nondiscrimination.** The Company values the dignity of each person as an individual and provides equal employment opportunities to all people based upon individual merit alone. The Company will not discriminate based upon race, religion, color, sex (which includes pregnancy, orientation, identification, expression, and all other legally protected characteristics), age, national origin, disability, veteran or military status, political beliefs, or any other characteristic protected now or in the future by applicable law. ***See*** **Equal Employment Opportunity**. We will not tolerate discrimination by any one with whom we do business.

- **Reasonable compensation.** The Company and our suppliers will pay reasonable compensation that, at a minimum, complies with all applicable laws and requirements.

- **Working hours and overtime.** The Company and our suppliers will comply with all applicable requirements and limitations set by the laws of the country of manufacture and may not require excessive overtime.

- **Compliance with U.K. Modern Slavery Act.** The Company and our suppliers will comply with the requirements of the U.K. Modern Slavery Act of 2015 and take steps to ensure that slavery, servitude, forced or compulsory labor, and human trafficking are not present in the Company or its supply chain.

- **The Company respects the right of workers to freely organize, associate, and bargain collectively in accordance with applicable national laws.** The Company and our suppliers will comply with the requirements of all national labor and employment laws.

Slavery is where ownership is exercised over a person; servitude involves the obligation to provide services imposed by coercion; forced or compulsory labor involves work or service exacted from any person under the menace of a penalty and for which the person has not offered himself voluntarily; and human trafficking concerns arranging or facilitating the travel of a person with a view to exploiting him or her.

If the Company finds any supplier to have violated the Act, the Company will promptly terminate its commercial relationship with that supplier.

- **Environment, health, and safety.** The Company is committed to sound environmental management, worker health, and overall safety. Safety awareness and procedures, waste minimization, and pollution prevention are primary objectives. ***See*** **Environmental, Health and Safety**. We expect the same commitments from our suppliers.

- **No bribery or corrupt payments.** Bribery of government officials or private persons is strictly prohibited. ***See*** **Anti-Bribery Policy (Appendix)**.

- **Antitrust and Fair Competition.** The Company and our suppliers are expected to comply with all fair competition laws and not engage in illegal monopolies, illegal behavior, price fixing, collusive bidding, price discrimination, and other unfair practices. *See* **Antitrust Compliance Manual (Appendix)**.

- **Intellectual Property.** Our suppliers must respect Sensient's and third party's Intellectual Property rights. Suppliers must promptly notify Sensient if they know or suspect that their products, or Sensient's use of their products, infringe any third party Intellectual Property rights.

- **Conflict of interest.** Our suppliers are expected to avoid and report all conflicts of interest resulting from their business dealings with Sensient and to notify Sensient if any Sensient employee has business, financial, or personal ties to the supplier that may influence such employee's decisions. *See* **Conflicts of Interest**.

- **Embargoes and Trade Law.** The Company and our suppliers shall comply with all applicable trade laws and restrictions imposed by the United Nations, the United States, and other national governments.

- **Property rights.** The Company and our suppliers will respect property rights and must ensure fair negotiation and compliance with all applicable laws and regulations on all land transfers.

Legal Services

The Corporate Legal Department will be responsible for providing Company management with guidance on all matters requiring legal interpretation, and for providing the Company with information pertaining to changes and developments in the laws affecting the Company business. Except as otherwise approved by the Chief Executive Officer, the Corporate Legal Department has the sole authority and responsibility to engage and supervise outside legal counsel. The Corporate Legal Department will keep the Company's operational departments involved and advised of pertinent developments in the law.

Manufacturing

The Company will manufacture safe products designed to satisfy customer needs and meet applicable legal requirements. The Company will assure the quality and legality of its products as they are distributed to our customers. Product and manufacturing specifications and quality control procedures will be established by operating units with advice and assistance from Corporate Engineering. All products will be manufactured in accordance with Good Manufacturing Practices. In cases where products are sold but not manufactured by the Company, suitable product quality guarantees from the outside supplier will be obtained, and the selling business unit will establish suitable quality control procedures. In addition, the following manufacturing protocols must be followed:

- Purchasing programs must be established to procure necessary manufacturing materials at the lowest cost consistent with quality and service standards.
- Maintenance programs must be established by business units to maintain physical assets used to manufacture, sell, and distribute products. Maintenance will conform to accepted or established engineering standards, encompassing proper measures for Employee safety, loss to fire or elements, explosion, etc.
- Programs must be established by business units to ensure proper compliance with all federal, state, and local regulatory codes regarding manufacturing and distributing food products in compliance with the **Product Safety** section of the Code.
- Business unit procedures, specifications, and programs are subject to review by Corporate Engineering.
- Inventories of raw materials, work-in-progress, and finished goods will be secured to prevent theft, unreasonable deterioration, or destruction.
- The security of the plant and equipment will be maintained at all times to prevent theft, unreasonable deterioration, and destruction.

- Insurance coverage specified by the Corporate Treasury Department will be in force at all times to protect the Company from undue loss.

Political Activities

Sensient does not make contributions to political candidates or parties. Employees may not make a political donation on behalf of Sensient, nor list their employment with Sensient in connection with any political activity, unless required to do so by applicable law. Nothing in this policy will be construed as limiting the ability of Employees to make political donations or engage in legal political activities in their personal capacities.

Product Safety

The Company takes pride in supplying our customers with products of the highest quality. Many of our products, including our food and beverage ingredients, cosmetic colors, fragrances, and pharmaceutical colors and flavors are intended for safe consumption or use by consumers. Our reputation and our ability to operate depend on our meeting this standard in everything we do.

Any Employee with concerns about the safety of Company products must immediately report that concern to his or her General Manager, who will notify the Company's Chief Executive Officer if the safety of Sensient's products is implicated. If the General Manager is unavailable or does not appropriately address the issue, an Employee must report the concern to the Company's Chief Executive Officer personally.

The Company is committed to provide only ingredients and products that are safe for consumers, properly labeled, and comply with all applicable requirements of law. This includes a commitment to comply with all food safety and labeling requirements of the Federal Food, Drug and Cosmetic Act (FDC Act), with all food safety and labeling regulations that have been issued by the U.S. Food and Drug Administration (the FDA) pursuant to the FDC Act, and with all applicable laws and regulations of the countries in which the Company sells products.

The FDC Act provides that all food (including food components) introduced into interstate commerce in the United States must be free of poisonous or deleterious substances that may be injurious to health; may not contain filth or otherwise be unfit for food; must be prepared, packed, and held under sanitary conditions whereby the food will not become contaminated or rendered injurious to health; and must include or provide only ingredients that are "generally recognized as safe" ("GRAS") for use, or that are food additives or color additives that have been approved as safe by the FDA. The Company is absolutely committed to compliance with all of these requirements for food safety and integrity, and all Employees are expected and required to perform their work in a manner that reflects unqualified commitment to these principals.

Media reports occasionally surface of contaminated or adulterated ingredients or raw materials from around the world making their way into food products. Product manufactured or supplied by the Company which does not meet all applicable safety and legal requirements should not be incorporated into any food or food component. Any decision to recall product manufactured by the Company must be made in accordance with the *Sensient Technologies Corporation Product Recall Manual,* and other applicable Company food safety manuals and guidelines.

Quality Audits

Periodic audits of our manufacturing facilities will be conducted to determine the state of facility compliance with good manufacturing practices and applicable laws and regulations. All such quality audits will be conducted at the direction of the Corporate Legal Department or the Audit Committee of the Board of Directors.

Terminations

All terminations of employment must be reviewed and cleared by the Corporate Legal Department prior to execution.

Waivers

Waivers or exceptions to the Code will be granted only in advance and only under exceptional circumstances. A waiver of the Code for any executive officer or director may be made only by the Board of Directors or a committee of the Board and must be promptly disclosed to shareholders in accordance with applicable law and New York Stock Exchange requirements.

Appendix

Antitrust Compliance Manual

Company Confidential Information Policy

Insider Trading Policy

Anti-Bribery Policy

Supplier Code of Conduct

Administration and Forms

SENSIENT TECHNOLOGIES CORPORATION
ANTITRUST COMPLIANCE MANUAL
2015

April 24, 2015

To All Sensient Employees:

We are committed to full compliance with every law and regulation that applies to our business. We take particular care to ensure we comply with the antitrust and competition laws in the United States and elsewhere. These laws are designed to protect and promote free and fair competition between companies. Because of these very broad purposes, these laws affect nearly every aspect of our businesses. Consequently, every Employee must have at least a basic understanding of the law and be able to spot antitrust issues when they arise.

An antitrust violation can carry severe consequences, including imprisonment, large fines, substantial damages awards, massive outside legal expenses, and general disruption of our businesses.

This Compliance Manual is designed to assist you in complying with the antitrust laws. Please study this Manual and consult it regularly during the course of your work. It will not turn you into an antitrust expert, but it will help you identify issues so that you may seek counsel from the Legal Department.

Employees who fail to comply with the law and this Manual will be subject to disciplinary action, up to and including termination. Under our Code of Conduct, we also expect every Employee to report any instance of non-compliance with the law and to inquire further when they become aware of any activity that might not comply with the law to the General Counsel. Employees who report actual or potential violations are protected from retaliation under the Sensient Code of Conduct.

Thank you in advance for your efforts to ensure that Sensient continues to maintain an outstanding record of compliance.

Sincerely,

Paul Manning
President and Chief Executive Officer

INTRODUCTION

Antitrust laws aim to promote and preserve competition among companies by outlawing actions that unreasonably restrict competition.[1] The justification for these laws is that free competition promotes consumer welfare by leading to lower prices, higher quality products and services, and more innovation. On the other hand, restrictions on competition can lead to higher prices, lower quality, and less innovation, all of which hurt consumers.

Although there are many laws, all antitrust laws aim to do two things:

(1) Prohibit agreements that unreasonably restrict competition (collusion); and

(2) Prevent companies that have market power from abusing that power through anticompetitive practices (exclusion).

All Sensient Employees must comply with all U.S. (federal and state) and international antitrust laws. No Employee or agent of Sensient has the authority to engage in, or direct another Employee or agent to engage in, any conduct that violates any antitrust law.

Any Employee with information about an actual or potential violation of antitrust law must immediately contact the Legal Department at 414-347-3777 or make an anonymous report using Sensient's Concerns Form located at http://sensus.sensient-tech.net/legal/SitePages/Home.aspx. Employees who do report actual or potential violations are protected from retaliation by the Sensient Code of Conduct.

Failure to comply with the law and this Manual, including a failure to report a known violation of the law, could result in criminal and civil penalties as well as disciplinary action, up to and including termination.

[1] For ease, we use the term "antitrust" to describe all laws that regulate competition.

DEALINGS WITH COMPETITORS

Antitrust laws prohibit agreements that unreasonably restrict competition. Most agreements between competitors, other than simple product sale or purchase agreements, will generally be found to unreasonably restrict competition and, therefore, will generally be found to be illegal.

Sensient is free to choose with whom it does business. But Sensient cannot make agreements with competitors that unreasonably restrict competition. Fortunately, sales of our products to a competitor or our purchases of a competitor's products will generally not be found to unreasonably restrict competition and, therefore, are generally permissible.

The term "agreement" includes all formal or informal agreements or understandings, whether written or oral. Given this broad meaning, any communication, at any level, between competitors can give rise to an inference that the competitors reached an illegal agreement. Given the legal risks, unless you are working to sell a product to or buy a product from a competitor, you must avoid verbal, written, or electronic communications with a competitor on any other matter.

Certain agreements with competitors are always illegal. You must **never** propose or make an agreement with a competitor to

- Set (fix) prices (high, low, or ranges);
- Limit production or capacity;
- Allocate geographic or product markets or customers;
- Rig or coordinate bids in a competitive bidding or RFP process; or
- Boycott or refuse to deal with a customer, supplier, or another competitor that is not party to the agreement.

Sensient will set its prices independently based upon our own internal analyses. In conducting our analyses, we may consider public source information about the prices charged by competitors, but we will never consult with competitors about pricing or any component of pricing. Also, Sensient will not make public announcements about pricing unless first approved by the CEO.

In our businesses we often buy from and sell to companies against whom we compete in one market or another. When we must communicate with a competitor for the sale or purchase of a product, the communications must be strictly limited in scope to the specific sale or purchase (e.g., price, specifications, and delivery terms) and also strictly limited in number.

You should never communicate with a competitor unless it is to discuss a sale of our products or a purchase of the competitor's products. You should never discuss any information that is not directly relevant to the specific sale or purchase.

Specifically, do **not** discuss the following with competitors:

- General market information
- Information about our businesses plans and finances;
- Our production capacity, costs, or plans;
- Our profit margins or pricing policies;
- Our suppliers or the prices we pay them;
- Our other customers or the prices we charge them;
- Our research and development plans;
- Other RFPs or bids; or
- Any other similarly sensitive competitive matters.

If a competitor ever attempts to engage you in a discussion about these sensitive topics, halt the discussion and immediately report the communication to the Legal Department.

Since trade associations, consortia, and standard setting organizations generally consist of competitors, these groups always raise serious antitrust concerns. Therefore, before joining or renewing membership in any trade association or consortium, or participating in a standard setting effort, consult with the Legal Department.

Trade shows also pose great antitrust risks. You should avoid contacts with competitors at trade shows.

Whenever you have questions about dealing with competitors call the Legal Department. You should submit all contracts to the Legal Department for review.

DEALINGS WITH CUSTOMERS, SUPPLIERS, AND DISTRIBUTORS

The antitrust laws also forbid agreements between companies and their vertical business partners that unreasonably restrict competition.

Antitrust issues can also arise in our dealings with customers, suppliers, distributors, and resellers ("vertical arrangements"). Because these issues can be particularly complex, contact the Legal Department before imposing competitive restrictions on customers, suppliers, distributors, or resellers.

The validity of such restrictions will depend upon their "reasonableness," that is, whether are they good or bad for competition. Reasonableness is assessed by analyzing the relevant market, our market power, the probable harmful competitive effects of the proposed restriction, and the probable benefits to consumers.

Examples of competitive restrictions that require Legal Department consultation include:[2]

- Setting minimum resale prices for distributors or resellers;
- Customer, territorial, and other non-pricing restrictions on distributors or resellers;
- Tying and bundling arrangements; [3]
- Exclusive dealing and requirements/output contracts; [4] and
- For commodities products, charging different prices to similarly situated customers.

MARKET POWER

Antitrust laws prevent companies that have market power from abusing that power.

Having market power means that we have the long-term power to raise prices and exclude competitors. Quantitatively speaking, market power generally means that sales of our product represent 50% or more of the sales in the relevant product or geographic market.[5] The question of when or if we have market power in the relevant product or geographic market is extremely complex.

A monopoly is an extreme form of market power, equating to control of at least 60-70% of the relevant market. It is illegal for a company to try to maintain or acquire a monopoly through predatory or exclusionary methods, that is, conduct that lacks a legitimate business justification and threatens to destroy or eliminate competition. But obtaining a monopoly by superior products, innovation, or business acumen is completely legal.

Again, Sensient is free to choose with whom it does business. But when we have market power, we must always be careful not to engage in predatory or exclusionary conduct. When we have market power, certain conduct may be considered predatory or exclusionary, including:

- Pricing below our cost to drive a competitor out of business;
- Tying using a product where we have market power or coercive bundling;

[2] As discussed below, when we have "market power," these actions are more likely to be considered unreasonable ("predatory" or "exclusionary") and therefore would be prohibited.

[3] Tying is where we require that a customer that wants to buy product A also buy separate product B. Bundling is where we only sell separate products A and B together, or provide a substantial discount if the customer buys both products A and B.

[4] An exclusive dealing contract is a contract that prohibits a purchaser from buying goods from a competitor, or prohibits a distributor from selling a competitor's products. A requirements/output contract is a type of exclusive dealing contract in which a customer commits to purchase all or substantially all of its requirements for a particular product from one seller, or a seller commits to sell all or substantially all of its output of a particular product to one customer.

[5] In the EU, the threshold for market power can be as low as a 35% market share.

- Exclusive dealings and requirements/output contracts that foreclose competition (e.g., an output contract for the entire market supply of an ingredient);
- Certain refusals to sell to a competitor (generally where we have monopoly power over a key ingredient or input); or
- Abusively using litigation or regulatory processes to increase the costs of competitors.

Always consult with the Legal Department concerning these issues.

OTHER PROHIBITED PRACTICES

The U.S. Federal Trade Commission Act prohibits unfair methods of competition and deceptive practices. The statute prohibits all of the conduct discussed above and the following:

- Commercial bribery;
- Coercion, intimidation, or scare tactics;
- False or deceptive statements about our products or a competitor's products;
- Stealing trade secrets; and
- Interference with other business relationships.

Accordingly, these practices are all prohibited by this Manual.

MERGERS AND ACQUISITIONS AND JOINT VENTURES

No Employee is authorized to discuss any prospective merger, acquisition, or joint venture without CEO approval.

CONSEQUENCES OF ANTITRUST VIOLATIONS

There are severe criminal and civil sanctions for antitrust violations. For U.S. criminal violations, individuals can be fined up to $1 million per violation and imprisoned for up to 10 years. Corporations can be fined up to $100 million per violation or twice the monetary gain to the defendant or twice the loss to the victim caused by the offense. When investigating offenses, U.S. law enforcement agents can use wiretaps, hidden cameras and recorders, confidential informants (usually company employees or business partners working with the government), or undercover law enforcement agents to build their case against a company.

For U.S. civil violations, prevailing plaintiffs can recover three times their actual damages. Civil cases can be pursued by government agencies, individuals, and companies. Civil cases can also be pursued as class actions, which means numerous plaintiffs can act together in one lawsuit. Damage awards can reach tens or hundreds of millions of dollars.

Civil plaintiffs can also seek court orders to bar anticompetitive conduct, both legal and allegedly illegal, to prevent competitive injuries to the plaintiffs. These court orders can often last for several years, severely hampering a company from competing effectively.

The legal fees associated with defending either a criminal or civil case can easily run into the millions of dollars. These cases generally last a number of years.

Company Confidential Information Policy

The protection of trade secrets and confidential information (collectively, "Company Confidential Information") is essential to the Company's capacity to develop products, provide services, and succeed as a business. Those who wrongfully acquire, misuse, or disclose CCI can cause significant damage to the Company.

A trade secret is information that is economically valuable because it is kept secret and is not easily ascertainable by outsiders. The holder of a trade secret must make reasonable efforts to keep the information secret. **In most countries, trade secrets are subject to specific legal protections. Violations of such laws can result in severe civil and criminal penalties.**

Examples of trade secrets include:

(1) scientific, technical, and engineering information such as methods, know-how, formulae, designs, compositions, processes, discoveries, improvements, inventions, computer programs, and research and development projects; and

(2) financial, business, and economic information such as information about business strategies and plans, production costs, purchasing strategies, profits, sales information, and customer and supplier information including product order histories, product need and preference information, product development information, product delivery schedules, pricing information, and lists of customers and suppliers.

Confidential information is other non-public, sensitive information which may not fall within the legal definition of "trade secret," but is nonetheless valuable because it is not known by others and efforts are made to protect it. Confidential information includes all non-public information that, if disclosed, might be of use to competitors or investors, or harmful to the Company, its customers or its suppliers. **Confidential information is protected by both law and contractual agreement between each Employee and the Company.**

During employment and any time after leaving the Company, Employees may not use or disclose any CCI without prior authorization of the Company. All Employees must also sign a written agreement (which may be part of a written employment agreement) pledging to protect CCI both during and after employment with the Company; however, the failure to sign such agreement will not relieve them of the duty to follow the obligations set forth in the Code of Conduct.

Nothing in this Policy prohibits Employees from:

(1) Reporting possible violations of federal or state law or regulation to, or participating in investigations by, any governmental agency or entity, including but not limited to the U.S. Department of Justice, the Securities and Exchange Commission, National Labor Relations Board, the Congress, and any agency Inspector General;

(2) Making other disclosures that are protected under the whistleblower provisions of federal or state laws or regulations; or

(3) For U.S. Employees protected by the National Labor Relations Act, exercising any Section 7 rights that they may have to communicate about working conditions.

Additionally, it should be noted, an Employee cannot be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that is (1) made in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and solely for the purpose of reporting or investigating a suspected violation of law; or (2) in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.

Finally, an Employee who files a lawsuit for retaliation by the Company for reporting a suspected violation of law may disclose the trade secret to his or her attorney and use the trade secret information in the court proceeding, provided that the Employee (1) files any document containing a trade secret under seal; and (2) does not disclose a trade secret, except pursuant to a court order.

Failure to adhere to the requirements of this Policy may result in disciplinary action, up to and including immediate termination.

General Rules

MARKINGS. When reduced to written or electronic form, all documents and files containing CCI must be marked "COMPANY CONFIDENTIAL." Notwithstanding this requirement, unmarked documents and files may still constitute CCI subject to this Policy and must be protected accordingly

DESIGNATION AUTHORITY. The highest ranking manager ("Senior Manager") at each of the Company's international business operations and locations, Company Officers and their designees have discretionary authority to designate information as CCI. Such authority will be exercised in a judicious and reasonable manner to assure the appropriate level of protection.

ACCESS. Access to CCI will be granted on a **need-to-know** basis only. An Employee "needs to know" CCI only when knowledge is necessary to perform a job-related duty. Senior Managers have final authority to grant access to CCI to Employees.

LIMITED USE. Employees must use CCI only as authorized and directed by, and for the benefit of, the Company. Employees may not use CCI for any purpose not related to the Company's business. Employees with access to CCI may not disclose such information within the Company to anyone that does not have a need to know such information.

DISCLOSURE TO NON-EMPLOYEES. Employees may not disclose CCI to non-employees without a written non-disclosure agreement approved by the Corporate Legal Department and a finding by the responsible Senior Manager that the non-employee has a specific need-to-know to the CCI.

THIRD-PARTY CONFIDENTIAL INFORMATION. Any trade secret or confidential information *received* by a Company Employee from a third party under a non-disclosure agreement must be protected as if it is CCI.

Employees are strictly prohibited from bringing to the Company a previous employer's trade secret or confidential information or otherwise disclosing or using such information in the course of employment with the Company.

RETURN OF INFORMATION. CCI belongs to the Company. Upon leaving the Company, or at the Company's request, an Employee must immediately return all CCI in his or her possession. Employees may not retain possession of any CCI when their employment with the Company ends.

Access through Computer Systems

Access to CCI contained within or accessible through computer or electronic communications systems ("computer systems") will be limited to those with a business need to access the information ("Authorized Users"). Senior Managers have the sole authority and responsibility for determining, approving, and documenting Authorized Users and their specific level of access to CCI.

The Corporate IT Department will be responsible for maintaining security systems, including firewalls, anti-hacking programs, anti-copying programs, and anti-virus programs, sufficient to safeguard CCI. Where practical, the Corporate IT Department will arrange for electronic files containing trade secrets to be encrypted.

Access to CCI will be controlled using a secure means of authentication, such as by use of passwords to confirm correct association with a username or account name.

Once computer access to relevant CCI is established, appropriate security mechanisms will prohibit an individual user from exceeding his or her authorized access.

CCI contained on designated high risk IT systems may not be removed, downloaded, or exported from such high risk IT systems without prior authorization from the Chief Information Officer. The Chief Information Officer has the authority to designate high risk IT systems and to notify all users of such designations.

When a new Employee reports for duty or there is a change in job responsibilities, his or her immediate supervisor will determine the Employee's need for a user account and the level of access required for the performance of the Employee's job. The supervisor will then send an appropriate request for such authorization and access to the Senior Manager for approval. Upon approval by the Senior Manager, the Employee's supervisor will

send the approved request to the person in the Corporate or local IT Department charged with creating user accounts.

Systems users must NEVER:

- allow anyone else to use their system privileges;
- share their user names or passwords with anyone else;
- exceed their authorized access;
- leave their IT systems unattended while CCI is accessible; or
- copy or transmit CCI to a non-Company computer system.

Systems users must secure their usernames and passwords to prevent unauthorized use, and must properly log out of systems when they have completed use. **System users may never leave their systems unattended while logged into any Sensient system with access to CCI.**

When any Employee leaves the Company, the local HR representative will notify the system administrator to arrange for immediate termination of the Employee's accounts upon his or her departure from the Company. The Corporate IT Department will establish a policy for retaining and analyzing the computers of departing employees to assess whether any CCI has been downloaded by the Employee prior to his or her departure from the Company.

Cyber Security

The Corporate IT Department will implement technologies and controls to prevent unauthorized access and use of the Company's computer systems and CCI. Each Employee will be trained no less than annually. Each Employee must use all mandated cybersecurity technologies and controls. Any misuse or circumvention of these technologies or controls is a violation of the Code.

Physical Security

The control of physical access to facilities where CCI is used or stored is extremely important to the Company's overall security program. Senior Managers will be responsible for ensuring the appropriate level of security and access control measures for their facilities. Senior Managers and immediate supervisors will also be responsible for determining the level of physical access required by each Employee. Senior Managers will conduct reviews of the physical security policies and regulations annually as well as whenever facilities or security procedures are significantly modified.

In accordance with the Code of Conduct, all visitors (including Employees from other sites) must sign in and out and provide government issued identification for inspection by Sensient staff upon arrival to a Company facility. Visitors will be escorted and monitored while on the Company's premises. Visitors also will receive and display a name tag, lanyard, or other identifying mark at all times during their visit.

Physical access to the hardware of computer systems containing CCI will be controlled and limited as directed by the Corporate IT Department.

Documents and electronic files not contained within computer systems (e.g., on flash drives) containing CCI must be properly secured at all times in a locked office, drawer, or safe. Such documents and electronic files may not be left unattended in an accessible location at any time.

Where feasible, a system (e.g., a physical log or computer security program) will be maintained for tracking access to documents or systems that contain trade secrets such as formulas, production processes, and new developments/inventions.

When any physical document containing CCI is no longer needed, it must be shredded. When any electronic file containing CCI is no longer needed, it must be properly deleted so as to be unrecoverable using ordinary means.

Annual Training

All Employees will receive annual training on this Policy as part of Code of Conduct training.

Audit

The Internal Audit Department will audit compliance with this policy as part of its regular audits.

Insider Trading Policy

It is a violation of both Company policy and of federal and state securities law for any officer, director, or other Employee of the Company to engage in any transaction involving Company stock when that officer, director, or other Employee is in possession of material, nonpublic information. Such illegal insider trading includes transactions entered into for the benefit of the individual *and* transactions entered into for the benefit of the Company. This policy also applies to material, nonpublic information relating to any other company with publicly-traded securities, including our customers, suppliers, or peer companies, obtained in the course of employment or association with the Company.

It is also both illegal and a violation of Company policy to communicate (or "tip") material, nonpublic information to others who may trade in securities on the basis of that information. Prohibitions on insider trading extend to the family members and individuals living in the households of officers, directors, and other Employees when those officers, directors, or other Employees are in possession of material, nonpublic information, as well as to neighbors and friends.

Company personnel or their tippees who trade on inside information are subject to severe civil penalties, criminal fines, and even jail terms. An officer, director, or other Employee who tips information to a person who then trades is subject to the same penalties as the tippee. It does not matter that the officer, director, or other Employee did not make the actual trade, nor that he or she did not profit from the tippee's trading.

What Information is "Material"?

All information that a reasonable investor would consider important in deciding whether to buy, sell, or hold securities is considered material. Information that is likely to affect the price of the Company's stock would almost always be considered material.

Examples of some types of material information include:

- financial results or financial forecasts for the quarter or the year;
- a major change in management or personnel;
- possible mergers, acquisitions, joint ventures, and investments in other companies;
- changes in relationships with significant customers;
- the gain or loss of an important contract, customer, or supplier;
- actual or suspected cybersecurity risks or incidents, including vulnerabilities and breaches;
- important product developments;
- governmental approval of major new products;
- major financing developments; or
- major litigation developments.

While these examples illustrate the types of information that would likely be considered material, the list is not complete. Questions regarding or any uncertainty whatsoever

concerning what sorts of information are material not addressed on this list should be directed to the Corporate Legal Department.

What Information is "Nonpublic"?

Nonpublic information is information that is not generally known or available to the public. One common misconception is that material information loses its "nonpublic" status as soon as a press release is issued disclosing the information. This is not true. In fact, information is considered to be available to the public only when it has been released broadly to the marketplace **and the investing public has had time to absorb the information fully.**

Examples of public disclosure include public filings with the SEC, Company press releases, and, in some cases, meetings with members of the press and the investment community, shareholders, and the public.

While the time it takes for the investing public to absorb information fully varies, as a general rule, information should be considered nonpublic until 24 hours after the information is released. Of course, if you are aware of any other material, nonpublic information at the time that 24-hour period has passed, you will still not be able to trade Company stock legally.

Keep in mind that any questioned transaction will be viewed with twenty-twenty hindsight, taking into account information that may only later become clear.

It is also important to note that, in general, regular, ongoing stock purchases associated with employee benefit plans such as the Company 401(k) plan will not be considered to constitute illegal insider trading. If, however, an officer, director, or other Employee were to re-allocate funds under such a benefit plan, he or she will be subject to Company prohibitions against illegal insider trading.

Trading in Other Securities

The Company may engage in business transactions with companies whose securities are publicly-traded. These transactions may include, among other things, mergers, acquisitions, divestitures, or renewal or termination of major contracts or other arrangements. Information learned in connection with these transactions or relationships may constitute material, nonpublic information about the other company. No officer, director, or other Employee may trade in the securities of these companies while aware of material, nonpublic information about such companies nor may he or she tip such information to any other person for such use.

In addition, business transactions of the Company may impact the publicly-traded securities of other companies that are economically-linked to the Company (i.e., peer companies). Therefore, no officer, director, or other Employee may use information learned through his or her employment or association with the Company to trade in the securities of such companies.

Consequences of Illegal Insider Trading

The Securities and Exchange Commission ("SEC") and the U.S. Department of Justice (generally through the U.S. Attorneys Offices) pursue insider trading violations vigorously and such violations are punished severely. While the regulatory authorities concentrate their efforts on individuals who trade or tip others who trade, the Federal Securities laws also impose potential liabilities on any company and its officers and directors, if they fail to take reasonable steps to prevent insider trading by company personnel.

Individuals who trade or who tip others who trade based on material, nonpublic information could face the following penalties **for each violation**:

- a return of any profits made on or losses avoided by, plus penalties of up to three times the amount of profits or avoided losses on, the illegal insider trading;
- twenty years' imprisonment; and/or
- up to $5 million in fines.

A company could face even stiffer penalties for a violation of insider trading laws, including up to $25 million in fines.

The existence of a personal financial emergency does not excuse an officer, director, or other Employee from complying with the Company's policies with respect to insider trading. Illegal insider trading, regardless of the justification, is still illegal.

Restrictions on Legal Insider Trading

Not all insider trading is illegal. Only trading that occurs on the basis of material, nonpublic information is illegal. However, because it is important to avoid even the appearance that trading has occurred based on material, nonpublic information, the Company has established the following set of policies that must be followed:

Window Periods

To limit the risk that Company officers and directors inadvertently violate insider trading laws, officers and directors of the Company are only permitted to trade Company stock during quarterly "window periods."

Each of these window periods begins 24 hours after the Company announces its annual and/or quarterly financial results for the prior fiscal year and/or quarter, and ends 30 calendar days after the beginning of the window period.

Notwithstanding the foregoing, the General Counsel will close an otherwise open window period for any officers, directors, and other Employees who know of a material event or information that is not generally known or available to the public, including the internal discovery of an actual or a suspected cybersecurity risk or incident.

Event-Specific Blackout Periods

On occasion, certain officers, directors, or other Employees may become aware of an event that is material to the Company that has not yet become public, including the internal discovery of an actual or a suspected cybersecurity risk or incident. Anyone with knowledge of such an event is prohibited from trading Company stock; in addition, the General Counsel may impose a blackout period during which those officers, directors, or other Employees who know of the material event, plus any other individuals who the General Counsel may designate, are prohibited from trading Company stock.

Because the very existence of a blackout period could signal to investors that a material event is pending, the Company will not announce, internally or publicly, that a blackout period is in effect; instead, the Corporate Legal Department will notify any officer or director who seeks pre-clearance to trade during a blackout period on an individual basis that a blackout period is in effect. No person made aware of a blackout period should disclose the existence of the blackout period to any other individual.

Trade Pre-clearance for Directors, Officers, General Managers, Business Unit Directors, Senior Financial Officers, and other Employees

The Company's directors, officers, general managers, business unit directors, Senior Financial Officers, and other Employees who assist the Company in the preparation of Reports or otherwise have a financial reporting oversight role, as well as any other individual making trades for the Company's account, are required to notify the General Counsel by e-mail or otherwise in writing of their intent to engage in any transaction involving Company stock. The General Counsel (or, in the General Counsel's absence, the Senior Attorney responsible for Securities matters) must pre-clear any trade by e-mail or otherwise in writing **at least two days** in advance of when the intended trade is to occur.

In order for a trade to be pre-cleared, the individual seeking pre-clearance must confirm to the General Counsel that he or she does not have knowledge of any material, non-public information and provide the General Counsel with the relevant terms of the proposed transaction, including what type of transaction is contemplated, the proposed terms of such transaction, the number of shares or other securities involved in the transaction, and who beneficially owns the securities.

The General Counsel (or, in the General Counsel's absence, the Senior Attorney responsible for Securities matters) will only pre-clear trades during a window period, when the General Counsel has not imposed a blackout period, and the General Counsel is not aware of any material, non-public information.

Once a transaction has been pre-cleared, it is Company policy that the intended trade take place (if at all) within two days of the grant of pre-clearance.

All records directly and materially relevant to pre-clearance will be retained for no less than five years.

Immediate Reporting of Trades by Directors and Officers

Federal insider trading laws require the reporting of transactions by officers and directors on a timely basis. Therefore, it is Company policy that once a transaction has been executed on behalf of an officer or director, that officer or director must immediately notify the General Counsel, by both telephone and by fax or e-mail, of the terms of the transaction. All reports will be retained for no less than five years.

The Company also requires officers and directors to notify any broker or dealer used to effect such transactions of the Company's reporting policies to ensure the broker's or dealer's cooperation with these policies.

Additional Trading Prohibitions

Company policy prohibits officers and directors of the Company from trading Company shares during any employee benefit plan blackout period except pursuant to a Rule 10b5-1 trading plan approved by the Company's board of directors as described below. The Company will notify officers and directors in advance of such blackout periods.

Rule 10b5-1 Trading Plans

Directors and officers who have entered into Rule 10b5-1 trading plans approved by the Company's board of directors need not adhere to the above requirements in the Code of Conduct regarding trade pre-clearance for directors and officers, window periods, or blackout periods with respect to trades occurring in compliance with the board-approved Rule 10b5-1 plan. However, directors and officers continue to have an obligation to follow the immediate reporting requirements outlined above.

Sensient Technologies Anti-Bribery Policy

Sensient Technologies Corporation is committed to conducting business ethically and in compliance with all applicable laws, including the United States Foreign Corrupt Practices Act ("FCPA"), the United Kingdom Bribery Act ("UKBA"), and the anti-bribery and anti-corruption laws of other nations.

This policy describes the Company's strict prohibition of bribery and other improper payments in the conduct of the Company's business operations. Compliance with this policy, the Code of Conduct, and all applicable laws is a condition of continued employment.

A bribe or other improper payment (in whatever form) is **never** acceptable. Moreover, it can expose you and the Company to possible criminal prosecution, steep fines, reputational harm, and other very serious consequences, including prison time. Remember: It is always better for the Company to suffer an economic loss than for one of its officers or employees to violate the law.

Sensient strictly prohibits bribery and other improper payments in all of its business operations. This prohibition applies to all business activities, anywhere in the world, and regardless of whether they involve government officials or are wholly commercial.

This policy applies to everyone who works for or with Sensient, including all directors, officers, employees, third party business partners, and other intermediaries that interface with government officials on the Company's behalf. We all have a personal responsibility and obligation to conduct Sensient's business activities ethically and in compliance with the law.

An intentional violation of an anti-bribery law is outside the scope of your employment with Sensient, and will result in automatic and immediate termination without notice or severance, regardless of your position in the Company. A negligent violation of this policy will result in disciplinary action, up to and including termination.

If you ever have any questions regarding this policy or its application to particular circumstances, you should contact Sensient's General Counsel.

FOREIGN CORRUPT PRACTICES ACT (FCPA) OVERVIEW

The FCPA contains two sets of provisions: the anti-bribery provision and the books and records provisions. The anti-bribery provisions prohibit covered companies and their employees from making corrupt payments to non-U.S. government ("foreign") officials to obtain or retain business.

The books and records provisions require covered companies to make and keep accurate books and records; to devise and maintain an adequate system of internal accounting

controls; and to prohibit knowingly falsifying books and records or knowingly circumventing or failing to implement a system of internal controls. The books and records provisions apply to bribery of foreign officials as well as to commercial bribery.

The FCPA applies to all employees of Sensient worldwide. The U.S. Department of Justice ("DOJ") and the Securities and Exchange Commission ("SEC"), which enforce the FCPA, interpret the law very broadly. While not necessarily accepting that these interpretations as binding or correct, this policy aspires to conform to or exceed these very broad interpretations.

The Anti-Bribery Provision

The FCPA anti-bribery provision prohibits:

● Corruptly paying, offering to pay, or authorizing the payment of, money or anything of value,

● directly or indirectly,

● to a foreign official

● in order to

· influence any official action or decision, or

· induce an official to perform/refrain from performing some act in violation of his or her lawful duties, or

· induce the official to use his or her influence to affect the act or decision of a government instrumentality, or

· secure any improper advantage,

● to assist the payor in obtaining, retaining, or redirecting business.

Payment of legitimate taxes, customs duties, licensing fees, and other legally mandated government fees does not violate the FCPA. To violate the FCPA, a payment to a foreign official must be made "corruptly." This means that the payment is made with a bad or wrongful purpose and with the intent to induce a foreign official to misuse his or her position.

> Example: The Company will pay all customs fees, duties, and tariffs as required by the laws of each nation in which it operates. The Company will **not** pay a particular customs official to secure an illegally reduced duty rate, or expedited customs clearance.

"Anything of value" includes cash, gifts, travel or entertainment expenses, charitable donations, and political contributions. The actual value does not matter. Both the DOJ and the SEC have stated that there is no minimum threshold amount.

A "foreign official" is anyone who exercises governmental authority at the local, state, or national level. Examples of foreign officials include:

(1) an officer or employee of, or any person acting in an official capacity for, any foreign government department or agency (example: customs official), or government owned or controlled instrumentality (example: an employee of a state-owned or state-controlled business enterprise);

   a. For purposes of this policy, **all** employees of companies that are owned in whole or part, or controlled by, a foreign government entity (whether national, state, or local, or executive, legislative, or judicial), are treated as "foreign officials."

   b. Bribery of such individuals constitutes bribery of a government official, commercial bribery, or both and is thus strictly prohibited.

(2) an official of a foreign political party (example, a Communist Party Official in China);

(3) any candidate for foreign political office; and

(4) any middleman for a foreign official described in subsections (1)-(3) above, such as associates, friends, and family members.

It is important to understand that the FCPA punishes intent, so it does not matter whether the payment is actually made, or merely offered. A mere attempt to make a payment is sufficient to violate the law. It also does not matter whether the official asks for the payment or someone else does. Furthermore, it does not matter whether the payment succeeds in getting the official to take action.

Significantly, as stated above, it does not matter whether the official is paid directly or indirectly, that is through a third party, such as an agent or consultant. Both the Company and individual employees can be held liable for the actions of other people ("third parties") taken on the Company's behalf. This is the case even if the third party is not subject to the FCPA.

> Example: The Company cannot authorize or permit a customs services agent working for the Company to pay a customs official in order to avoid a legally required duty.

Turning a blind eye or deliberate ignorance – **which includes not making a reasonable inquiry when there are suspicious circumstances** – is not a defense to an FCPA charge. In other words, we are all charged with making a good faith effort to control the actions of those who act on our behalf. We cannot just pay a third party to perform a service and hope they do not violate the law.

The Books and Records Provisions

The FCPA and other regulations require the Company to "make and keep books, records, and accounts, which in reasonable detail accurately and fairly reflect the transactions and dispositions of assets" of the Company. Misleading, incomplete, or false entries in the Company's books and records are never acceptable. Knowing falsification of books or records is a crime.

The FCPA and other regulations also require the Company to "devise and maintain" an adequate system of internal accounting controls sufficient to assure management's control, authority, and responsibility over the Company's assets. Knowingly circumventing these controls is a crime.

Significantly, the FCPA's books and records provisions do not have a materiality requirement. Thus, any violation, no matter how small, potentially subjects the employee and the Company to criminal and civil penalties. The U.S. government has charged both the employees who caused a foreign subsidiary to book bribes inaccurately and the parent company that incorporated the subsidiary's inaccurate records into its own financial statements.

Penalties

Each violation of the FCPA's anti-bribery provisions is punishable by up to five years in prison and up to a $250,000 fine for individuals and up to a $2 million fine for public companies. Each knowing violation of the books and records provisions is punishable by up to 20 years in prison and up to a $5 million fine for individuals and up to $25 million fine for public companies. Where an individual or company profited, or a victim suffered a loss because of the violation, the fines will be twice the total benefit obtained by the violator, or twice the total loss to the victim. A criminal fine imposed on an employee cannot be paid directly by his or her employer.

When the government pursues civil charges, there are also high monetary penalties. For an anti-bribery violation, the penalty is up to $10,000; for a books and records violation, the range is $5,000-$100,000 for individuals and $50,000-$500,000 for corporations. The SEC asserts that a company may not indemnify an employee for liability under the FCPA.

UNITED KINGDOM BRIBERY ACT (UKBA) OVERVIEW

The UKBA is more expansive than the FCPA. It prohibits:

- Offering, promising, or giving a bribe to another person;
- Requesting, agreeing to receive, or accepting a bribe from another person;
- Bribing a foreign public official; and
- For corporations: Failing to prevent bribery.

An act of bribery can be prosecuted where it is committed in whole or part by any person or entity in the U.K. or, if outside the U.K., by a U.K. citizen, a U.K. entity, or any other person with a close connection with the U.K.

Significantly, the UKBA also punishes "commercial organizations" that fail to prevent commercial bribery. A commercial organization is defined to include U.K. corporate entities/partnerships, as well as non-U.K. corporate entities/partnerships that carry on a business or part of a business in the U.K.

The corporate offense is a strict liability offense, which means if a bribe occurs, an organization can be liable, even if it has no knowledge of the offense, or the offense was committed by a third party acting on the organization's behalf ("associated person"). Fortunately, there is a complete defense if the organization had adequate procedures in place which were designed to prevent bribery by people associated with the organization.

If convicted of violating the UKBA, the maximum penalty is 10 years' imprisonment and an unlimited fine for an individual or corporation.

Few cases have been decided under the UKBA, which has created doubt about how it will be enforced. Because of this uncertainty and its potentially vast reach, Sensient will comply with the provisions of the UKBA everywhere it does business.

COMMERCIAL BRIBERY LAWS

The U.S. Criminal Code, the FCPA's books and records provisions, the UKBA, and most nations' laws prohibit commercial bribery. Commercial bribery is a corrupt payment to a private person made in order to obtain or retain business or other commercial advantage.

> Example: A salesperson at Company X offers to pay a purchasing agent at Company Y $1,000 if the purchasing agent agrees to ensure that Company Y buys Company X's products.

No Sensient director, officer, or employee may ever offer or agree to pay (or accept) a commercial bribe.

PERMITTED PAYMENTS

As stated above, the FCPA does not prohibit companies from paying lawfully required duties, tariffs, taxes, fees, and fines levied by foreign governments. Where possible, such payments should be made directly to the government agency, rather than to an individual government official, or through a third party business partner.

The responsible General Manager must ensure that those payments required by published legislative, administrative, or judicial order are paid and accurately documented in the Company's books and records. If you have any question about the legitimacy of a particular payment demanded by a foreign official, contact the Corporate Legal Department immediately.

PROHIBITED PAYMENTS

Examples of improper payments (i.e., bribes) to foreign officials include payments to illegally or improperly:

- Secure favorable tax treatment;
- Reduce or eliminate customs duties;
- Expedite the importation or exportation of goods or equipment;
- Expedite or enable the release of goods or equipment from customs;
- Circumvent a license or permit requirement;
- Influence a regulatory approval process;
- Obtain exemptions from regulations;
- Obtain government contracts;
- Gain access to non-public bid tender information;
- Influence a procurement process;
- Gain a business advantage; or
- Prevent competitors from entering the market.

If a foreign official ever asks you to make a payment beyond a legally mandated fee, **refuse to pay it**. Make it clear that your refusal is **absolute** and **unequivocal**. Immediately report the request to your supervisor and to the Corporate Legal Department.

Facilitating or Expediting Payments

Facilitating or expediting payments ("grease payments") are additional payments illegally made directly to a foreign official (usually in cash) to speed up a routine, non-discretionary government action. Although such payments are sometimes permissible under the FCPA, they are illegal under the UKBA as well as all national laws. Accordingly, illegal facilitating or expediting payments are strictly prohibited.

No director, officer, or employee may ever make, directly or through a third party, any illegal facilitating or expediting payment to any foreign official.

> Example: The Company cannot pay an immigration official to expedite the processing of immigration paperwork for a new employee.
>
> Example: The Company cannot pay a customs official to speed up the inspection process for the Company's products.

This section applies only to illegal payments to foreign officials. Where a government agency legally offers different speeds of service in their published rate schedule, it is permissible to pay the higher rate for faster service. Likewise, legal payments to a private entity to expedite a shipment are not prohibited (example: FedEx).

Gifts, Travel, and Entertainment Expenses

For Foreign Officials and U.S. Government Officials

No director, officer, or employee may ever provide, directly or through a third party, a gift to, or pay any travel or entertainment expense for, a foreign official or U.S. government official. A "Gift" means anything of value.

For purposes of this policy, a U.S. government official includes any employee of a local, state, or federal government department or agency in the United States.

> Example: A Company officer or employee may never give a gift to any employee of a company owned in whole or part, or controlled by a foreign government, regardless of the occasion, local practice, or local law.
>
> Example: A Company officer or employee may not pay the restaurant bill for a dinner with a customs official or an employee of a company owned in whole or part, or controlled by a foreign government.
>
> Example: A Company officer may not pay or offer to pay the travel expenses of an officer of a state owned enterprise who wants to visit one of our facilities.

No director, officer, or employee may ever provide a gift to, or pay any travel or entertainment expense for, any **other person** when such gift or payment is made with the intent to **influence** a foreign official or U.S. government official.

> Example: A Company employee may not give a gift to the spouse of a foreign official because it will appear that the gift was given to gain the goodwill of the foreign official.

These prohibitions apply to gifts or payments made directly or through a middleman.

> Example: A Company employee may not authorize its customs services agent to give a gift to a customs official on behalf of the Company.

The FCPA does permit reasonable, bona fide expenses directly related to the promotion of products, for example, presenting or demonstrating a product at a trade show. At such shows it is permissible to provide small items (under $20 USD value) such as a coffee mug, pen, or key chain to all customers and visitors.

> Example: A Company employee could hand out free hats to everyone who visits a Company booth at a trade show, without checking whether they are foreign officials.

It is also permissible to provide beverages and a light meal to foreign officials or U.S. government officials who visit a Company facility, provided that such beverages and light meals are routinely provided to all visitors. The General Manager of the facility will be responsible for properly documenting the visit and the provision of food and beverages.

> Example: A Company officer could offer coffee and pastries to the employee of a state owned enterprise who visits a Company facility to preview a new product. The General Manager must properly document the visit and what was provided to the visitor.

For Non-Governmental Customers and Business Partners

Because of the risk of appearance problems, we must exercise great caution when providing gifts and paying expenses for our non-governmental customers and business partners.

On limited occasions, with prior approval of the responsible General Manager, an officer or employee may give a gift to, or pay for the cost of a meal or other entertainment expense for, an officer or employee of a non-governmental customer or business partner. The value for a gift must be less than $100 USD (per person), and the value of the meal or entertainment expense must be less than $300 USD (per person), unless the General Counsel pre-approves a greater amount in writing. The gift cannot consist of cash or a cash equivalent (example: gift card). The gift should be given openly and transparently; provided only to reflect esteem or gratitude; permitted under local law and custom; and reasonable for the occasion. For meal and entertainment expenses, the Sensient officer or employee should be in attendance and pay the cost directly to the restaurant or entertainment venue.

Example: With prior approval, a salesman could present a retirement gift to the purchasing agent of a long-term commercial customer.

Example: The same gift would not be approved if the purchasing agent worked for a wholly or partially state owned or controlled enterprise.

With the prior written approval of the Group President, Sensient will pay directly for the travel and lodging expenses of non-governmental customers where the travel is related to the promotion of products (including related training).

Where travel expenses are directly related to the business partner's accomplishment of its obligations under a contract or engagement, prior approval is not required (example: a lawyer traveling to a deposition while representing the Company).

All gifts, meal and entertainment expenses, and travel expenses will be properly recorded in the Company's books and records.

Charitable Donations

Inside the United States, only the Sensient Technologies Foundation is permitted to make charitable donations on behalf of Sensient. Outside the United States, managers must get prior written approval from the General Counsel before making a charitable donation. Directors, officers, and employees may not make a donation on behalf of Sensient, nor identify themselves as an employee or representative of Sensient when making donations in their own name.

Political Donations

Sensient does not make contributions to political candidates or parties in any nation. Directors, officers, and employees may not make a political donation on behalf of Sensient, nor list their employment with Sensient in connection with any political activity in any nation unless required to do so under the laws of the nation in which the donation is made. Nothing in this policy may be construed as limiting the ability of directors, officers, and employees to make political donations in their personal capacities.

DUE DILIGENCE FOR THIRD PARTY BUSINESS PARTNERS THAT INTERFACE WITH FOREIGN OFFICIALS ON BEHALF OF SENSIENT

Sensient sometimes conducts business with or through a third party such as a contractor, consultant, vendor, distributor, reseller, lawyer, accountant, third party representative, customs clearance agency, freight forwarder, joint venture partner, or other intermediary ("third party business partner"). These relationships are important and provide valuable benefits in many areas of business. But these relationships can also present compliance challenges when the third party interfaces with government officials on our behalf.

Sensient will not do business with any person or company that will not abide by the law.

Because of the risks involved, Sensient will endeavor to enter written contracts with all third party business partners that interface with a government official on behalf of Sensient. Prior to engaging such a third party, the General Manager or his or her designee will endeavor to conduct due diligence in accordance with these principles:

● Complete anti-bribery questionnaire (Appendix A) and obtain an Anti-Bribery Pledge (Appendix B (third parties)) before the engagement and every three years thereafter;

● Request and receive Corporate Legal Department review and approval of any contract, or anti-bribery terms and conditions;

● Where possible, all payments for legitimate fees should be made by Sensient directly to the responsible government agency rather than through a third party business partner;

● Ensure all legitimate payments by a third party business partner to a government agency are explicitly documented and accounted for in the contract, invoices, and in our books and records;

● Review the qualifications and business reputation of the third party business partner;

● Ensure that the third party business partner is not owned in whole or part, or controlled by, a government;

● Determine whether the third party business partner employs individuals who are current foreign officials;

● Obtain and check the third party business partner's references;

● Check public sources. Do an open records search on the third party business partner, including criminal records checks of the company and its senior employees;

● Ensure the payment made to the third party business partner for its services is not above market price, padded, or steeply discounted;

● Ensure that any consultant engaged by the Company is in the specific line of business for which we have engaged him or her;

● Ensure the third party business partner is not related to, or closely associated with, any foreign official;

● Ensure we do not use a third party business partner recommended by foreign officials;

● Ensure that we do not pay a third party business partner in cash, nor make payments into offshore accounts or in any other non-standard or unconventional manner;

● Ensure all services to be provided by the third party business partner are detailed in a written contract or engagement letter, and costs are itemized and proportionate to the value of the services rendered;

● For high risk third parties such as consultants, include a contractual provision allowing Sensient to audit their books and records to ensure compliance with this policy;

● For real estate transactions, ensure Sensient has documentation of the fair market value of the property and that there are no foreign officials involved in the transaction (for example, as lessor, lessee, seller, or purchaser).

As part of the due diligence process a Sensient officer or employee will complete a due diligence questionnaire, and, where necessary, visit the third party's place of business. All due diligence efforts will be documented, including any adverse information that is discovered. All adverse findings (including refusals to answer questions) must be discussed with the Corporate Legal Department.

Each General Manager will be responsible for transmitting all due diligence records in .pdf to the Corporate Legal Department. The Corporate Legal Department will maintain a central database of all third party business partners that interface with foreign government officials on behalf of Sensient in order to track compliance with this policy.

Sensient will require all third party business partners to review this policy, and pledge to abide by all applicable anti-bribery/anti-corruption laws (Appendix B).

Ideally, all contracts with third party business providers who interface with foreign government officials on behalf of Sensient (or in the absence of a written contract, the terms and conditions of an order, agreement, or engagement) must contain the following terms:

● Indemnification: Full indemnification for any anti-bribery law violation, including all costs for the underlying investigation and any related litigation.

● Cooperation: Require full cooperation with any ethics and compliance investigation, specifically including the review of foreign business partner e-mails and bank accounts relating to its work for Sensient.

● Material Breach of Contract: Any anti-bribery law violation will be a material breach of contract, with no notice and opportunity to cure, and will be the grounds for immediate cessation of all performance and payments.

● No Sub-Vendors (without approval): Require agreement not to hire an agent, subcontractor or consultant without Sensient's prior written consent (which should be based on the same due diligence used for any third party business partner).

● Acknowledgment: Require acknowledgement of the applicability of the FCPA and any national or regional anti-corruption or anti-bribery laws relevant to the business relationship.

● Require that all persons performing services on our behalf review this anti-bribery policy, and annually certify (by signing Appendix B) that they will not engage in any conduct that violates the FCPA or any applicable anti-bribery laws.

● Re-qualification: Require the third party business partner to re-qualify as a business partner at a regular interval of no greater than every three years.

● Audit Rights: Require audit rights. These audit rights must exceed the simple audit rights associated with the financial relationship between the parties and must allow a full review of all anti-bribery law-related compliance procedures.

WATCH FOR WARNING SIGNS

As part of our due diligence process, and while our relationship with a third party business partner that interfaces with foreign officials on Sensient's behalf continues, all officers and employees must watch for signs that suggest a risk of potential corruption. Here are some common warning signs:

● They insist on unorthodox payment methods such as requesting payment be made in cash, to an offshore account, through another third party business partner, through a third country, or in a third country currency.

● They were specifically recommended by a foreign official.

● They refuse to agree to abide by, or violate, anti-bribery laws.

● They provide incomplete, inaccurate, or inconsistent disclosures.

● They request an unusually large commission in relation to the services provided.

● They request a "success fee."

● They request reimbursement for poorly documented or questionable payments.

● They request false or inaccurate invoices or documentation.

● They make unusually large or frequent political contributions.

● They have family or business ties to a relevant foreign official.

● Their only business qualification is influence over, or connection to, a foreign official.

This list is not exhaustive. Never ignore warning signs. Vigilance is critical. **When you see a warning sign, contact the Corporate Legal Department for advice and assistance.**

MERGERS AND ACQUISTIONS

The Corporate Legal and Internal Audit Departments will include an anti-bribery compliance review as part of their due diligence of any proposed merger, acquisition, or joint venture. The review will be in accordance with the principles outlined in this policy.

ANNUAL TRAINING

All directors, officers, and employees will complete an annual training program regarding this policy. Individuals involved in the selection, supervision, or contracting process with third parties that interface with foreign officials on behalf of Sensient will an additional annual training requirement concerning the specific requirements of their jobs. New hires will receive training as part of their orientation.

ANNUAL CERTIFICATION

Each director, officer, and employee, must sign an annual acknowledgement and reaffirmation of their responsibilities under the policy (*See* Appendix B). Each third party business partner (who interfaces with a foreign government official on behalf of Sensient) must sign such acknowledgement and reaffirmation every three years after first signing such acknowledgement.

Each President and General Manager will send these certifications to the Corporate Legal Department.

CONTACT REPORT REQUIREMENT

All Sensient directors, officers, and Employees must report to the Corporate Legal Department within 48 hours if they have any non-routine contact with any known or suspected foreign official. When in doubt, check with the Corporate Legal Department.

REPORTS OF VIOLATIONS OF THIS POLICY

Reports of violations or suspected violations of this policy must promptly be made to one's supervisor, an appropriate officer of the relevant subsidiary, or the General

Counsel. The Code of Conduct provisions regarding Reporting Possible Violations will apply in all respects. No employee will be penalized for making a report in good faith.

Employees of third party business partners must report any violations to Sensient's General Counsel.

AUDITS

As part of its regular audit duties, the Internal Audit Department will conduct a regular review of corporate books and records to ensure compliance with this policy. The Corporate Legal Department will assist the Internal Audit Department as necessary to evaluate overall compliance with this policy through monitoring of the central database of all third party business partners that interface with foreign officials on behalf of Sensient.

Where a third party business partner interfaces with a foreign official on behalf of Sensient in a nation that presents a high risk of corruption (defined as a ranking of 50 or higher on the most recent Corruption Perception Index), the Internal Audit Department will conduct a review of each such third party business partner no less than every 18 months, or whenever a contract is initiated or renewed, and then every 18 months thereafter. The Internal Audit Department will conduct a review of all other third parties that interface with foreign officials no less than every 24 months. The Internal Audit Department may retain local audit firms to assist in this process as necessary. A copy of the Internal Audit Department Anti-Bribery Checklist is provided in Appendix C.

ANTI-BRIBERY COMPLIANCE OFFICER

The General Counsel will be designated as the Anti-Bribery Compliance Officer. As such, he is responsible for enforcing and updating this policy, providing training, assisting directors, officers, and employees in complying with the requirements of the policy, and answering all questions concerning this policy. The Anti-Bribery Compliance Officer will also issue periodic updates to all employees regarding anti-bribery and anti-corruption issues.

The Anti-Bribery Compliance Officer will do an annual assessment of this policy and revise it as necessary to ensure its continued effectiveness, taking into account relevant developments in the field and evolving international and industry standards and practice. All revisions will be submitted to the Audit Committee of the Board of Directors for approval.

QUARTERLY REPORTS TO THE AUDIT COMMITTEE

The Anti-Bribery Compliance Officer will make quarterly reports to the Audit Committee of the Board of Directors regarding the Company's compliance with this policy and the need for any changes to this policy.

INVESTIGATIONS

The General Counsel, working in conjunction with the Internal Audit Department, will immediately conduct a thorough investigation of any reported or suspected violation of the FCPA, the UKBA, or any other applicable anti-bribery or anti-corruption laws.

Where the reported or suspected violation is corroborated by evidence sufficient to establish reasonable cause to believe that a violation may have occurred, the General Counsel will engage the assistance of outside counsel and outside auditors, and notify the Chairman of the Audit Committee.

RECORDS RETENTION

All records directly and materially relevant to compliance with this policy will be retained for no less than five years. The Anti-Bribery Compliance Officer may direct that particular records be retained for longer periods of time as he deems appropriate.

APPENDIX A

ANTI-BRIBERY QUESTIONNAIRE FOR ENGAGEMENTS WITH THIRD PARTY BUSINESS PARTNERS

DO NOT DISTRIBUTE TO THIRD PARTY BUSINESS PARTNER
MUST BE COMPLETED BY A SENSIENT EMPLOYEE

_____ Original _____ Update
(check one)

Name of Company:
Information about the Company:

What is the nature of its business?

How long has it been in business?

What are its qualifications?

What are some of its recent projects?

Company employees who will work or act on behalf of Sensient:

Describe all services to be provided by the Company and list the cost of each service:

Describe anticipated contacts with a government agency or entity on behalf of Sensient:

List anticipated costs or method of calculating costs of all legitimate payments to foreign government agencies (example: customs duties):

Can it be arranged for Sensient to make these payments directly to the foreign government agencies?

Does Company intend to use an agent or sub-contractor to fulfill its contractual obligations?

(If yes, you must complete a questionnaire for each sub-contractor or agent)

Is the Company owned in whole or part, or controlled by a government, or government employee/official? Explain.

Is any employee of the Company currently employed by a government in any capacity?
If yes, please list each individual and describe their employment:

Has the Company been involved in any lawsuits, enforcement actions, or government investigations for a violation of an anti-bribery law or for any other offense that involves dishonesty, corruption, or fraud? Explain.

Has any employee of the Company ever been convicted of violating an anti-bribery law or of any other law prohibiting dishonesty, corruption, or fraud? Explain.

Company has been provided with copy of Sensient's anti-bribery policy? _____ yes ____ no

Company has its own anti-bribery/anti-corruption policy? _____ yes ____ no

Contract with Company includes an anti-bribery provision? _____ yes ____ no

All Company officers and employees who work on behalf of Sensient have reviewed Sensient's anti-bribery policy and pledged to abide by its terms while working on behalf of Sensient _____ yes ____ no (attach pledges)

_____

Date(s) of discussions with Company to complete questionnaire: _____

Sensient Employee(s) participating in discussions:

Date(s) of visit to Company office/facility (if applicable): _____

Sensient Employee(s) participating in visit:

Attach a copy of any contract and all signed pledges to this questionnaire

Form completed by:

Date completed:

Date transmitted to Corporate Legal Department:

APPENDIX B (Employees)

PLEDGE TO ABIDE BY SENSIENT'S ANTI-BRIBERY POLICY AND ANTI-BRIBERY LAWS

Name: _____

Title: _____

Business Unit: _____

I have read Sensient's Anti-Bribery Policy. I am familiar with the policy and its requirements. I understand the provisions of the Foreign Corrupt Practices Act, the U.K. Bribery Act, and the general requirements of other anti-bribery laws as well as the consequences of violating such laws.

I understand that Sensient will pay all legally mandated government fees to the appropriate government agency in accordance with the law of each nation in which it operates.

I pledge that beyond legally-mandated payments, I may never offer, provide, attempt to provide, nor authorize or cause anyone else to provide, anything of value to any government official while working on behalf of Sensient.

I further pledge that I may never offer or pay or accept a bribe in any form.

If required to engage a third party business partner that will have contact with a government official or instrumentality on behalf of Sensient, I pledge to use my best efforts to exercise all necessary due diligence to ensure the third party will comply with the policy and all applicable anti-bribery laws.

If required to maintain books and records, I pledge to maintain those books and records fully, truthfully, accurately, and strictly in accordance with the law.

I understand that if I have any questions about Sensient's Anti-Bribery Policy, I may rely upon Sensient's Corporate Legal Department to assist me at any time.

I understand that Sensient's Anti-Bribery Policy requires me to immediately report all known or suspected violations of this policy to a supervisor or the General Counsel.

_____

Signature/Date

APPENDIX B (Third Parties)

PLEDGE TO ABIDE BY SENSIENT'S ANTI-BRIBERY POLICY AND ANTI-BRIBERY LAWS

Name: _____

Company: _____

I have read Sensient's Anti-Bribery Policy. I am familiar with the policy and its requirements. I understand the provisions of the Foreign Corrupt Practices Act, the U.K. Bribery Act, and the general requirements of other anti-bribery laws as well as the consequences of violating such laws.

<u>While working on behalf of Sensient</u>, I understand and pledge on behalf of myself and my company as follows:

I understand that Sensient will pay all legally mandated government fees to the appropriate government agency in accordance with the law of each nation in which it operates.

I pledge that beyond legally-mandated payments, I may never offer, provide, attempt to provide, nor authorize or cause anyone else to provide, anything of value to any government official.

I further pledge that I may never offer or pay or accept a bribe in any form.

I understand that if I have any questions about Sensient's Anti-Bribery Policy, I may rely upon Sensient's Corporate Legal Department to assist me at any time.

_____

Signature/Date

APPENDIX C
Internal Audit Department Anti-Bribery Policy Checklist for Internal Audits

General

Is the Sensient Anti-Bribery Policy posted in a conspicuous place in the facility?

Has every employee signed an acknowledgement and reaffirmation of their responsibilities under this Policy?

TPBP-Gs

Can the entity's leadership identify all third party business partners who interact with the government on behalf of the entity (TPBP-G)?

Has due diligence been conducted on each TPBP-G?

Review copy of completed anti-bribery questionnaire for each TPBP-G.

Is each questionnaire current (required every three years)?

Are there any red flags present in any completed questionnaire?
Has the person who interfaces with the TPBP-G observed any red flag behavior by the TPBP-G?

Does the entity have a signed Anti-Bribery Pledge from each TPBP-G?

Is the pledge current? (required annually)

Where permitted, does the entity pay legitimate government fees (taxes, customs duties, licensing fees, etc.) directly to the responsible government agency rather than through a TPBP-G?

If the entity is legally authorized to make direct payments, but does not, what is the justification?

Are legitimate payments by a TPBP-G to a government agency documented in the TPBP-G's invoice(s) and in the entity's books and records?

Are payments made to the TPBP-G for its services reasonable and in line with market prices (i.e., not above market price, padded, or steeply discounted)?

Ensure that we do not pay a third party business partner in cash, nor make payments into offshore accounts or in any other non-standard or unconventional manner.

Does the entity use consultants?

Is each consultant engaged by the entity in the specific line of business for which we have engaged him or her?

State Owned Enterprises

Does the entity do business with any state owned or controlled enterprises (SOEs)?

Does the entity properly treat SOEs as government entities?

Does the entity properly treat SOE employees (at whatever level) as government officials?

Gifts

Has the entity presented, or been requested to present, any gifts to any government official or SOE employee? (If yes, immediately report this to the General Counsel)

Was the gift properly documented in the books and records of the entity?

Has the entity presented any gifts to any commercial business partner?

Was each gift properly documented in the books and records of the entity?

For each gift over $100 USD, does the entity have documentation of prior, written approval from the General Counsel?

Was any gift a cash gift?

If yes, does entity have documentation of prior, written approval from the General Counsel? (If no, immediately report this to the General Counsel)

Meals, Entertainment, and Travel Expenses

Has the entity paid, or been requested to pay, for any meal, entertainment, or travel expense for any government official or SOE employee? (If yes, immediately report this to the General Counsel)

Was each meal, entertainment, or travel expense properly documented in the books and records of the entity?

Spot check books and records entries for routine meal, entertainment, or travel expenses paid for commercial business partners.

For meal and entertainment expenses over $300 USD, does the entity have documentation of prior, written approval from the General Counsel?

For travel expenses, does the entity have documentation of prior, written approval from the Group President?

Were travel expenses paid by a Sensient entity directly to the service provider (airline, hotel, etc.)?

Charitable Donations (non-U.S. entities only; all U.S. donations come from the Sensient Foundation)

Did the entity make any charitable donations in the last two years?

Is each donation properly documented in the entity's books and records?

Does the entity have documentation of prior, written approval from the General Counsel for each donation?

THE SENSIENT ANTI-BRIBERY POLICY:

Sensient will pay all legally mandated government fees to the appropriate government agency in each nation in which it operates. Beyond legally mandated payments, no director, officer, employee, or third party business partner acting on behalf of Sensient, may offer, provide, or attempt to provide, directly or through an intermediary, anything of value to any government official, or an employee of a wholly or partially government owned or controlled enterprise while working on behalf of Sensient.

The bribery of government officials or private persons in order to secure or retain business or other commercial advantage is strictly prohibited.

This Rule must be posted in a conspicuous location in every Sensient facility.

Supplier Code of Conduct

Sensient Technologies Corporation and our constituent companies strive to conduct business in an ethical manner and to make a positive contribution to society through our product offerings and business activities. We have a comprehensive Code of Conduct that governs all of our employees worldwide and seeks to inculcate a culture that promotes ethical behavior and compliance with all applicable laws and regulations. Complying with the law and observing our ethical obligations are absolutely essential conditions for fulfilling our duties to each other, our customers, and society as a whole. We expect the same high standards from our suppliers.

Sensient expects all suppliers, vendors, contractors, consultants, agents, and other providers of goods and services to adhere to the following principles.

Failure to comply with this Supplier Code of Conduct may be grounds for terminating the supplier relationship, and any relevant contracts, depending on the seriousness of the violation.

BUSINESS PRACTICES: Our suppliers must conduct their business lawfully and with integrity, including:

Compliance with all applicable laws and regulations. Our suppliers must comply with all applicable laws and regulations in the countries in which they operate.

Antitrust and Fair Competition. Our suppliers are expected to comply with all fair competition laws and not engage in illegal monopolies, illegal behavior, price fixing, collusive bidding, price discrimination, and other unfair practices. Our suppliers will not knowingly participate, directly or indirectly, in any agreement that unreasonably restricts competition. Our suppliers are also prohibited from abusing their market power through anticompetitive practices.

No bribery or corrupt payments. Sensient has a comprehensive Anti-Bribery Policy that requires behaviors that exceed the requirements of the United States Foreign Corrupt Practices Act and the United Kingdom Bribery Act as well as most local laws. Under these laws, suppliers are prohibited from corruptly paying, offering to pay, or authorizing the payment of, money or anything of value, directly or indirectly, to a foreign official in order to influence any official action or decision, or to obtain a business advantage. A "foreign official" is anyone who exercises governmental authority at the local, state, or

national level, and may include directors, officers, or employees of state-owned enterprises. Our suppliers must comply with these laws as well as our Anti-Bribery Policy while working on our behalf and be equally vigilant against bribery and corruption risks within their own organizations.

Intellectual Property. Our suppliers must respect Sensient's and third party's Intellectual Property rights. Supplier must promptly notify Sensient if supplier knows or suspects that supplier's products, or Sensient's use of supplier's products, infringe any third party Intellectual Property rights.

Cybersecurity. Suppliers will implement all necessary measures, and review them regularly, to protect their computer systems and networks. They will put in place appropriate controls to identify and mitigate relevant cybersecurity risks.

Protection of Confidential Information and Personal Information. Suppliers will comply with applicable privacy and data protection laws and ensure the protection, security, and lawful use of personal data and confidential information. In particular, the supplier must provide sufficient security for personal data and confidential information processing activities that concern the products or services provided to Sensient and ensure adequate technical and organizational protection measures are in place.

Conflict of interest. Our suppliers are expected to avoid and report all conflicts of interest resulting from their business dealings with Sensient and to notify Sensient if any Sensient employee has business, financial, or personal ties to the supplier that may influence such employee's decisions.

Gifts. Gifts to or from Sensient employees are neither expected nor necessary for business relationships between our supplier and Sensient. Our Code of Conduct prohibits Sensient employees from giving or receiving gifts of more than a token value, loans (other than from established banking or financial institutions), or hospitality or entertainment which could influence the employee's independent judgement, and all gift-giving is discouraged. These prohibitions apply to gifts or payments made directly or through an intermediary.

Affiliation with Governments and Government Officials. Our suppliers must immediately disclose to Sensient any affiliation in regard to ownership or beneficial interest in a supplier's business by a government or government official of more than 5%. These must be disclosed to Sensient prior to any business relationship or immediately after supplier becomes aware of such interest; provided that if a supplier is a publicly listed company, supplier shall only be required to disclose to Sensient any such ownership or beneficial ownership interest if the supplier has actual knowledge of any such ownership.

The following are examples of persons who may be considered government officials:

- Any officer or employee of a foreign government, regardless of rank;
- Employees of government-owned or government-controlled businesses;

- Foreign politicians, political parties, or candidates for office; and
- A family member or agent of the above.

Embargoes and Trade Law. Our suppliers shall comply with all applicable trade laws and restrictions imposed by the United Nations, the United States, and other national governments.

Management and Transparency. Our suppliers are expected to have systems in place to track compliance with applicable laws and regulations and to investigate, to the extent allowed by law, allegations of misconduct. Suppliers must immediately inform Sensient in writing if they are aware of any material noncompliance with local laws involving either the supplier or a Sensient product. **Responsible sourcing**. Our suppliers must disclose the country of origin for the primary materials for all deliveries made to Sensient. Sensient reserves the right to ask suppliers for a full supply chain map in order to facilitate risk assessments and gauge legal and ethical compliance in the upstream supply chain. Our suppliers will be transparent about all known facilities used to produce products or services for us and provide such information upon request. If requested, suppliers are expected to provide reports on the presence of substances in any materials supplied to Sensient that may be restricted by, or require disclosure to, governmental bodies, customers, and/or recyclers.

Conflict minerals. Our suppliers must report the presence of conflict minerals (as defined by 15 U.S.C. § 78m(p)), including whether the conflict minerals originated in the Democratic Republic of the Congo (DRC) or adjoining countries, in the products they manufacture or contract to manufacture if the conflict minerals are necessary to the functionality or production of a product. Sensient initiates an annual due diligence review process of our supply chain to ensure that products supplied to Sensient do not contain metals derived from minerals or their derivatives originated from conflict regions that directly or indirectly finance or benefit armed groups and cause or foster human rights abuses.

WORKFORCE PRACTICES: Our suppliers are expected to provide a safe workplace, which operates in compliance with all applicable laws, and to treat their employees lawfully, respectfully, and fairly, including:

Human Rights. Our suppliers must respect and support global human rights. Global human rights are fundamental to the operations of Sensient's business. Human rights are rights, freedoms, and standards of treatment regarded as belonging to all persons. Sensient respects and supports internationally recognized human rights and is committed to high standards of ethics, honesty, and integrity and demonstrating respect and dignity for one another and those with whom we do business.

No forced labor or trafficking. Our suppliers are prohibited from using slaves or forced labor of any kind, including prison labor, non-rescindable contracts, indentureship, or labor obtained through threats of punishment, deposits of bonds or travel documents, or other constraints, or engaging in human trafficking. If applicable, supplier is expected to

have filed a transparency statement in compliance with the UK Modern Slavery Act 2015.

No child labor. Our suppliers are prohibited from employing children under the age of 15 years (or any higher age established by applicable law). Suppliers will conform to Convention 138 (Minimum Age) and Convention 182 (Worst Forms of Child Labor) of the International Labor Organization.

No harassment or abuse. Our suppliers are prohibited from harassing or abusing employees. Our suppliers must treat their employees with respect and dignity, and without harassment or abuse of any kind. To the extent permitted by law, suppliers must strive to provide a workplace free of any form of harassment, intimidation or victimization, whether physical, psychological, or sexual.

Nondiscrimination. Our suppliers must provide equal employment opportunities to all people and will not discriminate based upon race, religion, color, sex (which includes pregnancy, orientation, identification, expression, and all other legally protected characteristics), age, national origin, disability, veteran or military status, political beliefs, or any other characteristic protected now or in the future by applicable law.

Diversity and inclusion. Our suppliers are expected to value the dignity of each employee as a unique person with individual skills and perspectives. Suppliers are expected to categorically reject individuals and ideologies that seek to sow hate, discord, and division based upon an individual's personal characteristics. Suppliers should strive to unite themselves with their employees by focusing on their common humanity and by dedicating themselves to the principles of integrity, professionalism, and safety.

Reasonable compensation. Our suppliers will pay reasonable compensation and benefits that, at a minimum, comply with all applicable laws and regulations.

Working hours, overtime, and wages. Our suppliers must comply with all applicable requirements and limitations set by the laws of the country of manufacture and may not require excessive overtime. Overtime must be voluntary and must always be paid at the statutory rate. Employees must be provided sufficient time each week for rest. Our suppliers must provide employees with wages and benefits that, at a minimum, comply with applicable law.

Workplace health and safety. Our suppliers must provide a safe workplace for their workers including, at a minimum, adequate lighting, ventilation, potable water, and sanitary facilities. Where required or appropriate, suppliers must provide safety equipment, guards, and protective clothing/masks to protect workers from hazardous machinery and materials, fire suppression and evacuation protocols, and security measures to ensure employees' safety while on or entering or exiting Supplier's premises.

Respect the right of workers to freely organize, associate, and bargain collectively in accordance with applicable national laws. Our suppliers will comply with the

requirements of all national labor and employment laws, including all union, freedom of association, and collective bargaining laws.
Sensient will not tolerate any violation of these principles.

ENVIRONMENTAL PRACTICES: Our suppliers must treat the environment with respect, including:

Environmental compliance. At a minimum, our suppliers will conduct their businesses in compliance with all applicable laws in a way that minimizes impact to the environment. As practical, suppliers should seek to reduce their environmental impact beyond what the law currently requires.

Hazardous waste management. Our suppliers must capture, contain, and dispose of all hazardous wastes safely and in accordance with all applicable laws.

Air quality and carbon footprint. Our suppliers will take appropriate steps to minimize air emissions (including carbon emissions) and impact on air quality, as far as possible and put in place practices to assess and reduce their emissions (including carbon). Suppliers will provide documentary evidence of their carbon footprint and their efforts to reduce it, if requested.

Energy efficiency. Our suppliers will take appropriate steps to minimize the consumption of energy as well as put in place energy saving strategies (i.e., use of renewable sources and fuels, fuel-efficient logistics operations).

Water management and conservation. Our suppliers will take appropriate steps to minimize their impact on water by reducing their water consumption, by ensuring groundwater quality is maintained and (where possible) improved, and by supporting water conservation. We also expect our suppliers to take appropriate steps to provide documentary evidence of their water usage assessment if requested.

No deforestation. Our suppliers will take appropriate steps to ensure their actions avoid negative impacts on forests, peatlands, and other protected areas. When establishing new operations or expanding existing ones, our suppliers shall obtain all legal approvals and permissions. We also expect our suppliers to keep documentary evidence of land use history and provide it if requested.

COMMUNITY PRACTICES: Our suppliers must treat the communities they are in with respect, including:

Property rights. Our suppliers must respect property rights in the communities in which they operate and must ensure fair negotiation on all land transfers to which they are a party, including free, prior, and informed Consent for new developments.

Health and safety impact. Our suppliers will seek to prevent and adequately address any adverse health and safety impact of their operations on surrounding communities.

Indigenous people. Our suppliers will respect the rights of local communities and indigenous people and their cultural heritages.

Local sourcing. Our suppliers will seek to employ and source goods and services locally whenever practicable.

CONTINUOUS IMPROVEMENT: Our suppliers must continuously improve their operations and methods.

We recognize that achieving the requirements of this Code is a dynamic process and we encourage continuous improvement within a supplier's operations. In cases where improvement is required, we will support our supplier to establish clear milestones and processes to support their achievement. Our suppliers who fail to comply with the requirements of this Code may be subject to consequences up to and including termination of business.

VIOLATION REPORTING: Our suppliers will encourage and provide means for their employees to report concerns, complaints, or potentially unlawful activities in the workplace, with the option to do so anonymously, without threat of reprisal, intimidation, or harassment.

Any report should be treated in a confidential manner. Suppliers shall investigate such reports and take corrective action if needed. Suppliers shall notify Sensient of legal actions, administrative investigations, or prosecutions that may affect their performance of any contractual obligations to Sensient, or where such legal actions could adversely affect a supplier's or Sensient's reputation.

> If at any time a supplier or one of its employees believes that a Sensient employee has acted contrary to these principles, the supplier or its employee is encourage to report its concerns to our Compliance Hotline at 1-414-347-3897 or supplierconcerns@sensient.com.

DECLARATION OF COMPLIANCE

Suppliers declares the following:

- Supplier has read and understands the Sensient Supplier Code of Conduct (Update 2021).
- Supplier agrees to comply with the Sensient Supplier Code of Conduct (Update 2021) while working with Sensient.
- Supplier agrees that Sensient reserves the right to terminate any agreement or business relationship with any supplier that cannot demonstrate compliance with our Supplier Code of Conduct.
- Supplier undertakes to improve or correct any identified deficiencies. Where applicable, Sensient may require corrective action and the implementation of continuous improvement plans as a condition of doing business.
- Supplier agrees that Sensient reserves the right to assess and/or monitor compliance with this Code, where applicable through a third party, and in any way (reasonable on-site inspections, questionnaires, interviews, etc.).
- Supplier agrees to conduct due diligence throughout its supply chain on its employees, agents, subcontractors, suppliers, and sub-suppliers to the extent they are involved in the provision of goods and/or services to Sensient to ensure compliance with this Supplier Code and applicable law.

On behalf of Supplier:

_____ _____

Title Date

ADMINISTRATION AND FORMS

Administration

The Code of Conduct (the "Code") was established at the direction of the Board of Directors and has the unqualified support of the Board and the Company's Senior Management. To ensure proper communication of Company policies and proper implementation of the Code, the Corporate Legal Department reviews the Code from time to time. Its responsibilities include:

- Establishing and interpreting the Code.
- Reviewing the Code to ensure it is adequate and revising and updating it as appropriate.
- In conjunction with the Human Resources Department, overseeing Company-wide education, communication, training, and new employee orientation programs.
- In conjunction with the Internal Audit Department, monitoring and auditing practices and procedures to ensure compliance.
- In conjunction with the Internal Audit Department, investigating possible violations.

The Corporate Legal Department reviews the foregoing activities with the Chief Executive Officer and makes periodic reports to the Board of Directors as appropriate.

Distribution and Training

The Code will be distributed to all Employees. During orientation, Employees will be introduced to the Code and educated about their responsibilities for complying with the Code. All managers and department heads will be responsible for reviewing the Code with their Employees to ensure the Code is fully understood. The Company will also provide Employees with ongoing training. The type and content of training will vary, depending upon an Employee's position within the Company.

Before an Employee leaves the Company, an exit interview may be held to reinforce the Employee's obligation to continue to comply with the Code to the extent that it applies to former Employees. Also, the exit interview may be used to elicit information about improper activities which the Employee may have been unwilling to disclose while working for the Company.

The Company may use additional methods to distribute information regarding the Code. In all cases, the Company's primary objective is to educate Employees about legal and ethical requirements and to reinforce the policy that improper behavior will not be tolerated.

All Employees are required to sign the *Code of Conduct Statement and Questionnaire* when first hired. This requirement also covers Employees who join the Company through an acquisition. Employees will be trained periodically on selected sections of the Code. Documentation of such training will be maintained by the Company.

Monitoring Compliance

Internal systematic reviews of practices and procedures will be conducted throughout the Company. These reviews may include management reports, internal audits, management reviews, and Employee interviews.

Periodic internal audits will be conducted throughout the Company by the Internal Audit Department in conjunction with the Corporate Legal Department, as appropriate. Audits will include evaluating compliance with policies, procedures, and regulations, reviewing the quality and integrity of financial statements, and reviewing internal controls of new and existing management systems. Results of these audits will be presented to Senior Management and the Board's Audit Committee, as appropriate.

FORMS

Initial Employment Statement

SENSIENT TECHNOLOGIES CORPORATION

Code of Conduct Statement and Questionnaire

Please complete each section on both sides of this form. Then sign and date the form and return it to your human resources representative.

1. I, _____, hereby declare and certify that I have read the Sensient Technologies Corporation Code of Conduct (the "Code"). I have abided and will abide by the Code's provisions during my employment with Sensient Technologies Corporation (the "Company") or its subsidiaries. I realize that failure to observe and comply with the Code's provisions will be a basis for disciplinary action, including dismissal.

2. To the best of my knowledge, neither I nor any dependent member of my family has or has had any interest or taken any action which could cause a conflict of interest as described in the Code, except as stated below. The exceptions are (if none, write none):

3. To the best of my knowledge, all Company operations in which I am involved are in compliance with the Code and have prevented violations of law, including (among others) preventing bribery or corruption as described in the Code, except as stated below (if none, write none):

4. I declare that my immediate family and/or I do not own in excess of 5% of the stock of any business, enterprise, company, or partnership whose shares are listed on public security exchanges/markets or regularly traded over the counter which does business or competes with the Company or its subsidiaries, except as listed below (if none, write none):

Stock Date of Purchase

5. I declare that my immediate family and/or I directly or indirectly do not own any interest (other than listed or publicly traded securities) in any entity which does business or competes with the Company or its subsidiaries, except as listed below (if none, write none):

Organization Ownership Interest Date of Purchase

6. I declare that my immediate family and/or I have the following family relationships with Company Employees or any relationships (other than those reported under statements 4 and 5) with persons, organizations, or enterprises that do business with or compete with the Company or its subsidiaries or which proposes to do so (if none, write none):

Relationship Date of Commencement

7. I will immediately report any future relationships, interests, transactions, and arrangements of the kinds listed above and in the Code, as they arise during the course of my employment with the Company or its subsidiaries.

8. I will immediately report violations of laws, rules, regulations, or the Code to appropriate personnel. I know that the Company will not allow retaliation for reports made.

_____

Employee Signature

_____

Position Department Location

_____

Date

(Prepare in duplicate, forwarding original to the director or manager of human resources for your business unit. Keep the copy for your personnel files.)

SENSIENT TECHNOLOGIES CORPORATION

Code of Conduct Certificate

*Read the Sensient Technologies Corporation **Code of Conduct** carefully. Then complete this form and return it to your human resources representative.*

As an employee of Sensient Technologies Corporation (the "Company") or one of its subsidiaries, I hereby state that I have carefully reviewed the Company's Code of Conduct which outlines the Company's general requirements and policies of business conduct, including the Company Confidential Information Policy, and the Sensient Anti-Bribery Policy.

I acknowledge the continuing effectiveness of the Company's Code of Conduct. I realize that failure to observe and comply with the Code's provisions will be a basis for disciplinary action, including dismissal. I will immediately report violations of laws, rules, regulations, and the provisions of the Code to appropriate personnel. I know that the Company will not allow retaliation for reports made.

In signing this I certify that I am not aware of any violations of laws, rules, regulations, or any provision of the Code of Conduct, except as follows: [if none, write NONE]

_____
Signature

_____
Print name

_____
Position Department Location

_____
Date

_____
Supervisor/Witness

Reminder
Statement

_____
Date

SAMPLE

SENSIENT TECHNOLOGIES CORPORATION

Request for Approval to Serve on Other Boards

To: Corporate Legal Department
Sensient Technologies Corporation
In accordance with the Company's Conflict of Interest Policy, I hereby request approval to serve as a member of the board of directors or as an officer of:

Name of organization: _____
Position: _____
Term: _____
Signature: _____
Date: _____
Print Name: _____
Position: _____
Department: _____
Location: _____

SAMPLE

SENSIENT TECHNOLOGIES CORPORATION

Request to Meet Competitive Situation

1. Customer Name and Location:
2. Product:
3. Quality:
4. Competitor:
5. Price/Terms that the Company must offer to meet – not beat – competitive situation:
6. Date of offer to Customer
7. The Company's regular Price/Terms for this product:
8. Has the Customer threatened to terminate purchase, cancel order refuse to place an order unless competitive pricing is met? _____ Yes _____ No
9. Name of the Company representative receiving competitive information:
10. Customer representative conveying this information:

Before deviating from standard pricing and/or terms to meet a competitive situation, describe the nature of the competitive offer and attach verification/explanation as required below. Remember that exceptions to standard pricing and terms may be made only to meet – not beat – a competitive offer.

11. Date, time, place, and circumstances under which competitive information was conveyed:
Proof of existence of competitor's offer – Circle One (attach if in writing):

A. Competitive data from customer (i.e., competitor's, sales invoice, discount schedule, or price list).
B. Note from customer setting forth competitor's offer (should be signed and dated).
C. Reports of similar offer made to other customers in the area.

12. Additional comments (e.g., explanation if no written confirmation attached):

Do not communicate with competitors to verify competitive practices under any circumstances.

Approved by:

Date: