Our Corporate Creed

Sensient Technologies Corporation is committed to conducting a business enterprise which is of real and continuing value to society. This requires bringing together, in an optimal manner, shareholders, employees, suppliers and civic resources so that customers are well served, profits are fairly earned in the competitive marketplace, investors are rewarded, employees grow in their careers, and the needs of the community are recognized by the appropriate commitment of corporate time and wealth.

Our Commitment to Ethical Standards

General Policy and Procedures for Business Conduct 3
Reporting Possible Violations 4
Consequences of Violations.....6
Accounting Matters…….....6
Antitrust Laws.....8
Antiboycott Laws.....9
Bribery.....9
Communicating Extraordinary Matters to the CEO 9
Communications with Analysts and the Media 10
Company Property……10
Confidentiality.....10
Conflict of Interest.....10
Director Confidentiality Policy……12
Document Retention 13
Electronic Communications.....14
Environmental, Health and Safety. 16
Equal Employment Opportunity.....17
Export Controls — USA.....18
Facility Visits.....18
Fair Dealing 19
Foreign Corrupt Practices Act and Other Anti-Corruption Laws 19
Fraternization Policy……....20
Government Inspections, Inquiries & Investigations 20
Harassment 21
Insider Trading 22
Inventions 24
Legal and Ethical Compliance.....25
Legal Services.....26
Manufacturing.....26
Political Activities.....27
Product Safety……..27
Waivers……28

Administration

Distribution and Training.....29
Monitoring Compliance.....30

Appendix

Antitrust Laws.....31
Company Confidential Information Policy……..…37
Insider Trading.....41
Anti-Bribery Policy.....45
Code of Conduct Statement & Questionnaire.....66
Code of Conduct Certificate (Reminder Statement).....68
Request for Approval to Serve on Other Boards 69
Request to Meet Competitive Situation.....70
Code of Conduct Glossary.....71

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. It is the policy of the Company to conduct its business as a good corporate citizen and to comply with all laws and regulations applicable to its business. 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 this Company.

This 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. This Code is not an employment contract, and the Company may modify or repeal the provisions of this Code or adopt a new Code at any time it deems appropriate, with or without notice.

This Code replaces the Standards of Conduct for International Employees, the Code of Ethics, and the Procedures for Reporting Complaints or Concerns Regarding Accounting, Auditing or Other Compliance Matters.

All Employees are responsible for understanding this 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 this 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 this Code. Employees are required to promptly report violations of law and/or of this 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 this 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

If any Employee believes the Code has been violated, he or she shall promptly report the matter to the Vice President, Administration, the General Counsel or the Assistant General Counsel. 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 http://intranet/finance/governance.htm. 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 shall cooperate in the investigation of suspected violations.

Consistent with all applicable national laws, all reports of violations will be promptly investigated and remedied as appropriate under the direction of the Vice President, Administration and the General Counsel.

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 Vice President, Administration, General Counsel, Internal Audit and/or 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 shall retain as part of its records all reports of complaints or concerns regarding Compliance Matters and their treatment. The Vice President, Administration will assist the Audit Committee by maintaining files regarding all reports, tracking their

receipt, investigation and resolution and shall prepare a periodic summary report thereof for the Audit Committee.

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

The Vice President, Administration and the Corporate Legal Department will conduct periodic reviews of reports, 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 either a company's internal compliance and reporting system or a government official or 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 this Code of Conduct 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 this Code of Conduct 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 this Code

of Conduct shall be construed to prevent an Employee from communicating with any government agency regarding matters that are within the agency's jurisdiction.

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.

This 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 with and make certain submissions (the "Reports") to the Securities and Exchange Commission and the New York Stock Exchange and disseminate them 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 are (i) 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://intranet/finance/controllersmanual.htm. It is the responsibility of local, division 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.

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 Corporate 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 of 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 shall 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

Most governments have enacted a series of antitrust or competition laws that aim to help consumers by preserving competition in the marketplace, thereby increasing output and/or reducing prices for consumers. It is essential that Employees have a basic understanding of the types of conduct prohibited by the antitrust and competition laws. Employees must be extremely careful in their dealings with competitors of the Company, and must immediately report any questionable activities or suspicious contacts with competitors to the Corporate Legal Department. The Corporate Legal Department can help determine whether particular conduct is of the sort prohibited by the antitrust or competition laws or by this Code of Conduct.

As a general matter, any agreement with a competitor that restrains competition is illegal. Several types of agreements have been determined to injure competition such that they are normally considered unlawful. This category includes agreements to fix prices, rig bids, boycott a supplier, limit production and agreements to allocate customers, markets or product lines. The Company's prices must be set independently by the Company without consultation of any kind outside the Company.

Never discuss prices or pricing with a competitor. Additionally, never discuss any Company Confidential Information with a competitor unless there is an approved non-disclosure agreement in place as required by the Company Confidential Information Policy. ***See*** **Company Confidential Information Policy.**

Additionally, certain rebates, price discounts and purchase incentives can sometimes violate antitrust and competition laws. Before any Employee offers, negotiates or agrees to such arrangements, he or she must discuss the arrangement with the Corporate Legal Department.

U.S. federal antitrust laws are typically complemented by similar state laws. Although there are exceptions, compliance with U.S. federal antitrust laws will usually constitute compliance with state laws. In addition, many foreign countries as well as the European Union also have antitrust or competition laws. While some of these laws are similar to the U.S. antitrust laws, others are significantly different. As a rule of thumb, where the Company does business outside the United States, Employees should assume that conduct prohibited by the U.S. antitrust laws is also prohibited by the competition laws of that country.

The U.S. antitrust laws provide for both civil and criminal penalties. They are enforced both by government agencies and by private parties. Companies and individuals who lose private antitrust suits can be required to pay three times the amount of the damages proven by the plaintiff, plus the plaintiff's attorneys' fees. This could amount to millions of dollars. In addition, if a court finds the conduct criminal, an individual could be

convicted of a felony, sentenced to jail for up to 10 years, and fined up to $1 million. The Company could be fined as much as $100,000,000 or more.

The Appendix to this Code of Conduct provides a more detailed summary of the types of conduct prohibited by the federal antitrust laws. Employees are not expected to be experts in these laws, but they are expected to be able to recognize when potential problems may exist and immediately seek guidance from the Corporate Legal Department

Remember: Employees are required to report any questionable activities or suspicious contacts with competitors to the Corporate Legal Department for appropriate follow-up.

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.

Bribery

***See* Anti-Bribery Policy**

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 shall 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 and other investors and investment professionals. As a result, except as otherwise designated by the Company's Chief Executive Officer, the Vice President and Chief Financial Officer or the Vice President and Treasurer are the only authorized contacts for discussions with investors, investment professionals and/or 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 and/or securities analyst.

Except as otherwise designated by the Company's Chief Executive Officer, the 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 shall protect the Company's property and assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on the Company's profitability and are prohibited.

Any suspected incident of fraud or theft should 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 shall 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 a size as to have influence or control over the corporation).
- **Gifts.** Employees and their family members shall 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. 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.
- **Loans**. The Company will not extend, maintain or arrange for any personal loan to or for any director or elected 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 are much more than our equipment, inventory, corporate funds or office supplies; they 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 which 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.

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 shall not disclose Confidential Information unless they first obtain the express permission of the Board.

Accordingly:

- no director shall use Confidential Information (as defined below) for his or her own personal benefit or to benefit persons or entities outside the Company, including other shareholders;

- no director shall discuss Confidential Information, specific potential or actual Company business operations or transactions with anyone outside of the Company, including other shareholders;

- no director shall discuss Confidential Information in public settings or other settings where inadvertent disclosure may occur;

- no director shall 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; 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. The Company expects all Employees to 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 shall not engage in or tolerate the making or using of unauthorized software copies under any circumstances. Employees shall 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 shall 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 shall 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 and positive interactions 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

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 Company-owned or operated facility shall comply with all applicable local, state and federal environmental, health and safety ("EHS") laws and regulations. All Company facilities shall be operated in a manner to avoid harm to human health or the environment, prevent pollution and reduce waste generation.

All Employees will be appropriately trained and are expected and required to perform their job 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, or 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 policy, standards and initiatives related to Company activities which may impact the environment or employee health and safety. This Department oversees environmental, health and safety compliance matters at every facility, and has full access to all Company facilities, records, property and personnel relating to EHS matters. 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 EHS compliance audits at designated Company facilities.

Group or Division Presidents, General Managers and Plant / Facility Managers
Group or Division Presidents are responsible for ensuring compliance with applicable federal, state and local laws and regulations and for implementation of Corporate EHS policies and associated procedures at their respective facilities. Plant/Facility Managers are responsible for day-to-day compliance with Corporate EHS policies and procedures and for developing and implementing programs to ensure that each activity, facility, source or condition attains and maintains compliance with applicable EHS laws and regulations. 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 facility compliance.

EHS Audits
Periodic audits will be conducted to determine the state of facility compliance with applicable EHS laws and regulations. All EHS audits shall 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.

Equal Employment Opportunity

The Company will provide equal employment opportunities to all people without discrimination because of their race, religion, color, sex, age, national origin, disability, veteran or military status, or any other characteristic protected by state, federal or local law (collectively, "protected classes"). The Company will administer all policies, benefits

and programs, including but not limited to interviewing and selection, compensation, promotion, transfer, layoff, recall, and training, on a nondiscriminatory basis.

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.

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

Export Controls - USA

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.

In general, the Company may not conduct any transactions directly or indirectly with any individual or company in Cuba, Iran, North Korea, Syria, Sudan, and Burma (aka Myanmar). Obviously, this means we cannot sell directly into, or buy directly from, the embargoed countries. It also means we cannot sell our products to another company (manufacturer or distributor) if that company will re-sell our products into one of the embargoed countries. And we cannot buy products from any company where the products originated directly or indirectly from one of the embargoed countries.

In very specialized cases, some Company products can only be sold with a license from the U.S. Departments of State or Commerce.

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 either an embargo or licensing requirement.

Facility Visits

Facility visits by customers, suppliers or other non-employees are sometimes necessary. Because of the confidential and proprietary nature of our processes, access to Company facilities by non-employees should be controlled and should comply with the procedures outlined below. Visits by the employees of state-owned or -controlled businesses are subject to the provisions of the **Anti-Bribery Policy (Appendix)**.

- Any visitor must be accompanied at all times by a Company Employee.
- Facility visits by customers must be approved in advance by the General Manager or Managing Director.
- Suppliers will not be permitted to visit facilities unless a business purpose is established (e.g., regular sales call for locally purchased supplies, inspection of equipment, etc.).

- The general public will not be allowed plant visits. In special cases, such as academic personnel or overseas visitors, the General Manager or Managing Director may approve a facility visit.
- All facilities shall maintain a log of facility visitors as provided in the Corporate Record Retention Policy. The log shall also contain appropriate notice of the confidentiality of Company operations or information at the facility, and shall clearly indicate that by "signing-in," the visitor agrees to maintain such confidentiality. No non-Employee visitor is to be allowed access to any Company facility or office unless they "sign in" prior to entry and receive a "Visitor" pass, which they must display at all times while present in Company facilities.
- Facility visits should be structured so as to avoid areas containing Company Confidential Information unless the visitor "needs to know" that information and has signed an appropriate non-disclosure agreement. ***See*** **Company Confidential Information Policy**

The Company prohibits Employees from visiting competitor plants as well as certain other sensitive competitor facilities such as laboratories and distribution or research centers without the prior approval of the Group or Division President. Approval of the Group or Division President is also needed for visits by competitors to Company facilities. The Chief Executive Officer, Chief Operating Officer, or Group or Division President may also approve specific exceptions to this policy in connection with corporate development and other Company activities. The Chief Executive Officer, Chief Operating Officer or Group or Division President may also approve specific exceptions to this policy if necessary to accomplish industry-wide projects involving public policy or the public interest such as safety, industry standards and environmental controls.

Fair Dealing

Every Employee shall 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), Senior Managers and human resources 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 Corporate Human Resources Department. 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 he *Governmental Inspections Manual* 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.) shall immediately communicate such information to his or her responsible Plant, Facility or General Manager or Managing Director. 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 or Managing Director shall immediately notify the Corporate Legal Department of the inquiry or investigation. The Corporate Legal Department shall 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 shall immediately refer such requests to the Corporate Legal Department, and no Company information shall 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 seeks to provide a work environment that is free from intimidation and harassment based on race, religion, color, sex, age, national origin, disability, genetic, veteran or military status, or any other characteristic protected by any applicable local or national law. The Company specifically prohibits such intimidation and harassment.

Sensient does not tolerate workplace violence. Accordingly, any Employee who is determined to have assaulted, battered, or threatened any person shall be terminated.

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) which 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; 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 shall **immediately** report it to the Vice President, Administration.

Harassment or similar unacceptable activities that could become a condition of employment or a basis for personnel decisions, or which 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 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 been the subject of prohibited harassment or retaliation, the Employee should first speak to the person who has engaged in the inappropriate behavior about his or her conduct, provided the Employee does not feel in danger and is comfortable doing so. The offensive conduct may have been thoughtless or based on a mistaken belief that it was welcome. If the inappropriate behavior does not stop or if the Employee is not satisfied with the result of the discussion with the offender or if Employee is not comfortable speaking to the offender directly, the Employee should report the inappropriate conduct as provided for in this Code, as stated under *Reporting Possible Violations*, as soon as possible. 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 this Code of Conduct.

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 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 stock of our customers, suppliers and even competitors.

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 stock in the Company, 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 or the entering into or loss of a major Company contract 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.
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 shall 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 shall engage in transactions in Company securities only during the Company's trading "window period," which is described in the Appendix to this Code of Conduct.
- No director, officer or other Employee shall 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 this Code of Conduct 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 shall 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 shall 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. Employees shall not circumvent the application of these laws. Neither the Company nor its Employees shall assist any third party in violating the laws of any country.

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 shall nevertheless establish employment practices and shall 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 Vice President, Administration or the Corporate Legal Department. ***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 prohibited, including prison labor, non-rescindable contracts, or labor obtained through threats of punishment, deposits of bonds or other constraints.

- **No child labor.** Work by children under the age of 15 years (or any higher age established by applicable law) is strictly prohibited.

- **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 will provide equal employment opportunities to all people without discrimination because of their race, religion, color, sex, age, national origin, disability, veteran or military status, or any other characteristic protected by applicable law. ***See* Equal Employment Opportunity**. We expect the same from our suppliers.

- **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.

- **Environment, health and safety.** The Company is committed to sound environmental management, worker health and 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).**

Legal Services

The Corporate Legal Department shall 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 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 division 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 divisions 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 divisions 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 this Code.
- Division 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 shall 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 shall 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 and 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 shall immediately report that concern to his or her General Manager, who shall 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 shall 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) and with all food safety and labeling regulations that have been issued by the U.S. Food and Drug Administration (the FDA) pursuant to that 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 shall be free of poisonous or deleterious

substances that may be injurious to health; shall not contain filth or otherwise be unfit for food; shall be prepared, packed and held under sanitary conditions whereby the food will not become contaminated or rendered injurious to health; and shall 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 shall be conducted at the direction of the Corporate Legal Department or the Audit Committee of the Board of Directors.

Waivers

Waivers or exceptions to the Code of Conduct 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.

Administration

This Code of Conduct 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 this Code, the Corporate Legal Department reviews this 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 Audit Department, monitoring and auditing practices and procedures to ensure compliance.
- In conjunction with the 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 Corporate 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.

Appendix

ANTITRUST LAWS

Antitrust and competition laws can be exceedingly difficult to apply to particular situations. This appendix is intended to be a brief introduction to the many issues that may arise under such laws. It is intended to help managers spot potential issues so they may seek counsel from the Corporate Legal Department.

U.S. federal antitrust laws can apply worldwide. Here are the primary U.S. laws:

The **Sherman Act** makes two types of behavior illegal:

- Section 1 of the Sherman Act prohibits any agreement that unreasonably restrains trade or commerce; and
- Section 2 of the Sherman Act prohibits any company from illegally monopolizing or attempting to monopolize any segment of trade or commerce.

The **Clayton Act** prohibits conduct that may tend to restrict competition in the sale of goods. This statute provides more detail than the Sherman Act. For example:

- Section 3 of the Clayton Act generally prohibits "exclusive dealing"—selling products to a customer on the condition that the customer will refrain from buying competitors' products;
- Section 3 also prohibits a company from selling its products on the condition that the customer buys other products from that company. This conduct is typically referred to as a "tying arrangement"; and
- Section 7 of the Clayton Act prohibits mergers of companies that tend to restrict competition or create a monopoly.

The **Robinson-Patman Act**—which is part of the Clayton Act—prohibits (1) price discrimination when selling products to competing customers, and (2) favoring one competing customer over another in providing promotional allowances and services.

Finally, the **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.

Who is a competitor?

How the U.S. antitrust laws are applied to Sensient's communications with another company will vary depending on the nature of our relationship with the other company. When the other company is a customer or supplier, it is obviously necessary to talk about the price and terms of the particular transaction taking place with the other company. Similarly, when Sensient is collaborating with another company on a joint project, it may

be necessary to discuss price and terms as they relate specifically to the project. Even if the other company may be a competitor in another setting, such discussions are permissible **if limited to the transaction involved**. But, as outlined below, discussions with competitors about prices and terms of sales to others outside the context of a collaborative project are generally illegal.

Prohibited competitor contacts

Meetings, conversations, and other contacts with employees of the Company's competitors are often commercially, professionally, or socially proper. However, competitor contacts pose substantial antitrust risks. Under the antitrust laws, it is illegal for competitors to agree on competitive matters. The term "agree" refers to an agreement in any form, whether oral or written, express or implied. Agreements and concerted action among competitors can result when there are frequent and informal contacts among them.

Agreements among competitors on the following topics are prohibited by the antitrust laws:

Pricing. Although all antitrust violations are serious, the most serious are price-fixing agreements among competitors, which are *per se* illegal—that is, they are illegal no matter how justifiable they may seem or how insignificant their market impact. They include agreements among competitors to decrease, as well as increase, prices; to stabilize prices; to set a formula for computing prices; to set price differentials; and to set minimum or maximum prices. In fact, an agreement on pricing is illegal even if the prices agreed upon are not uniform or no exact price is set. It does not matter that the agreed upon prices are reasonable, or that the purpose of a price agreement is to prevent ruinous competition. It is still illegal.

Agreeing to elements of price or to terms of sale, such as discounts, freight charges, or credit, is just as illegal as agreeing to the price itself. **Never discuss prices or pricing policy with a competitor.**

The following rules of conduct should be followed carefully:

- If a competitor attempts to discuss prices, stop the conversation immediately and telephone the Corporate Legal Department.
- Never provide to, or accept from, a competitor a price list or information from which prices can be computed. While price lists of competitors may be obtained from customers, customers should not be used as a clearinghouse for exchanging price information. Note the date and source of any competitor price information obtained from a customer on the face of the material.

Allocation of territories or customers. It is illegal for competitors to divide or allocate territories in which they will sell. Never agree with a competitor to sell or to refrain from selling in any area.

It is illegal for competitors to divide or allocate the customers to whom they will sell. Never agree with a competitor to sell or to refrain from selling to any customers or class of customers, or to divide or share a customer's business with a competitor.

Agreements to limit or restrict production. An agreement among competitors to restrict or limit production is illegal.

Boycotts and refusals to deal. An agreement between competitors not to sell to or buy from certain individuals or firms is illegal. Never suggest that a competitor, supplier or customer should not sell to or buy from anyone.

Bidding practices. An agreement between competitors to prevent genuine competitive bidding, such as an agreement not to submit a bid, or to submit a "low-ball" bid, is illegal.

Permissible competitor contacts

While Employees must avoid discussions with competitors that would lead to the types of unlawful agreements discussed above, the following types of contacts with competitors are proper when limited to their intended purposes:

- Selling our products or services to competitors;
- Purchasing competitors' products or services;
- Business collaborations approved by the Corporate Legal Department;
- Sharing historical account information for credit purposes or legitimate background investigations in accordance with privacy and other laws;
- Meetings of professional societies and trade associations;
- Meetings or communications concerning pending legislation or regulatory actions;
- Participation in civic, educational, or charitable organizations in connection with their proper activities;
- Participation in activities not directly related to the Company's operations, such as attending general business seminars; and
- Personal relationships with employees of competitors strictly as friends or neighbors, with no discussion of the prohibited topics discussed above.

Trade association activities

Because trade associations are, by definition, combinations of competitors, participation in trade associations requires special sensitivity to the Company's policy of strict compliance with the US antitrust laws. Company Employees should seek and maintain membership only in those associations that serve a valuable business purpose and that are sensitive to antitrust concerns. Prior to joining an association, Employees shall consult with the Corporate Legal Department regarding potential antitrust risks Be especially attuned at association meetings to discussions which might raise antitrust risks.

Refusals to Deal and Exclusive Dealing

A seller, such as the Company, is generally free to choose its own customers and to unilaterally "refuse to deal" with any person or company, absent an illegal purpose for the refusal.

The term "exclusive dealing" means an arrangement in which a manufacturer requires its customer to handle or buy only its products and not to handle or buy products made by the manufacturer's competitors. Because such an arrangement may violate the antitrust laws, it is unwise to suggest or imply to a customer that the customer must handle Company products exclusively or drop a competitor's product in favor of Company products.

While exclusive dealing arrangements may raise antitrust concerns, that does not mean that the Company is in any way prohibited from attempting to obtain, through lawful means, as much of its customers' business as it can.

Unilateral Action Regarding Distributors' Prices

A manufacturer, such as the Company, may take certain unilateral action regarding the prices its distributors charge when they resell the manufacturer's products. For example, the Company may establish and publish suggested list prices and urge its distributors to charge those prices. The Company may go further and establish a policy that it will refuse to deal with distributors who do not follow the suggested list prices and announce that policy to its distributors. A manufacturer with such a policy may refuse to engage in any further dealing with a distributor who fails to comply with the policy. However, the communication informing a distributor that the manufacturer will no longer deal with it must be limited to stating that fact. Conduct or communications that go beyond this could result in an agreement by the distributor to comply with the policy. At that point, the manufacturer's action is no longer unilateral, but involves an agreement between two parties – the manufacturer and the distributor – on price. Such an agreement will be regarded as unlawful unless it satisfies the "rule of reason" described in the next section.

Agreements Regarding Distributors' Prices

The law regarding price-fixing agreements among competitors was discussed earlier. The law regarding agreements as to resale prices (prices charged by a distributor) changed over time. Previously, it was *per se* unlawful for a manufacturer and its distributor to agree even on the minimum price the distributor would charge when it resells the manufacturer's products. Whether such an agreement encouraged competition was not relevant under prior law.

Now, such agreements are examined under the facts and circumstances of a particular situation using the so-called "rule of reason." Under the rule of reason, some agreements as to minimum resale price may be judged lawful because, on balance, they encourage competition. An example is where the manufacturer's business strategy calls for aggressive marketing activity and customer education by its distributors. The incentive for distributors to engage in such activity can be destroyed if price-cutting distributors

who do not engage in such activity can swoop in and make the sale after all the groundwork has already been laid.

Rule of reason analysis continues to apply to agreements regarding the maximum resale price to be charged.

Because analyzing the legality of a resale price agreement under the rule of reason can be difficult, no agreements with distributors regarding resale prices should ever be entered into without explicit clearance from the Corporate Legal Department.

The Rule against Discrimination in Price and Promotional Allowances

The U.S. antitrust laws prohibit price discrimination in the interstate sale of goods. The federal price discrimination law, known as the Robinson-Patman Act, generally requires that a manufacturer who sells products of "like grade and quality" to customers who compete with one another in the resale of the product charge them the same price for that product. This anti-discrimination rule applies not only to the price of the product itself, but also to such terms of sale as credit terms and freight allowances. The same terms generally must be offered to all competing customers.

Furthermore, promotional services or allowances such as advertising allowances must be offered to all competing customers on proportionally equal terms. Exclusion or improper treatment of a customer can result in illegal discrimination against the disfavored customer.

These general anti-discrimination rules may or may not apply in particular circumstances. Price discrimination violates the law if it creates at least a reasonable possibility that the price difference harms competition. Where the favored and disfavored customer(s) are not competitors in the resale of the product, a price difference is unlikely to harm competition and thus is unlikely to violate the Robinson-Patman Act.

In addition, to violate the Robinson-Patman Act, the sales at different prices must occur at about the same time. It is the date of the pricing decisions, not the date of delivery of the products, which is important.

Finally, even if competitive harm and other conditions necessary for a price discrimination violation exist, a price difference may still be lawful in certain circumstances. In the case of discounts to customers based on large-volume purchases, if such discounts are available to all customers who would be willing to purchase that large volume of goods, then the discount program is legal.

Also, when a customer tells a manufacturer that a competitor is offering a lower price, the manufacturer may lawfully lower its price to that customer to meet (but not beat) its competitor's price. To rely on this defense, the manufacturer must have a good-faith basis for believing that the competitor is charging a lower price – e.g., an invoice or a memorandum recording the word of a trusted customer. The claim of a lower competitive price must never be verified by direct or indirect contact with the competitor.

Tying Arrangements

A “tying arrangement” or “tie-in” occurs when a manufacturer’s offer to sell a product or service is conditioned on the customer’s purchase of other products or services from the manufacturer. “Full-line forcing” occurs when a manufacturer requires the customer to purchase an entire line of its products. These arrangements can be illegal. Do not force a customer to buy additional unwanted products. Any proposed agreement or arrangement calling for the mandatory purchase of more than one product or service as a package or group must be reviewed and approved in advance by the Corporate Legal Department.

Monopolization

The Sherman Act prohibits monopolization and attempts to monopolize. A company which is sufficiently dominant in its market is involved in monopolization when it tries to control through exclusionary or unfair means a large enough portion of a market so that it can control prices or output in that market. It is impossible to list all practices that, when pursued by a dominant firm, may result in monopolization charges. But, some examples of such practices include:

- Localized price cutting to eliminate a competitor;
- Selling below cost for the purpose of injuring a specific competitor;
- Attempts by a manufacturer to close distribution channels to rivals by demanding that distributors deal only in the manufacturer’s products; or
- Creation of marketing programs targeting a particular competitor or its customers.

Inaccurate or boastful references to the Company’s “share of market” or to “dominance in a market” may create a misleading impression of market power to antitrust enforcement authorities or plaintiffs’ lawyers.

The Company does not “control,” “dominate,” or “own” any market. Such words or similar phrases shall not be used in presentations, correspondence or internal memoranda. Such misleading references may create the false impression of monopoly power even though the Company has no such power. Instead of using the terms “market” or "share of market," it would be better to use terms like “segment,” “industry,” “area,” and “share of sales in that segment.”

Predatory pricing

Selling a product below cost can be illegal. There is no hard-and-fast rule as to what constitutes a price “below cost.” In calculating pricing, both the price to the customer and any credits or promotional allowances offered in a particular sale should be taken into account. As a very general rule, prices should at least cover average variable cost. Another general rule is that the higher the Company’s share of a particular market, the higher the chance that Company pricing will come under scrutiny.

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 shall 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 shall not relieve them of the duty to follow the obligations set forth in this Code of Conduct.

None of the provisions in this Policy 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.

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 **shall 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 shall have discretionary authority to designate information as CCI. Such authority shall be exercised in a judicious and reasonable manner to assure the appropriate level of protection.

ACCESS. Access to CCI shall 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 shall have final authority to grant access to CCI to Employees.

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

DISCLOSURE TO NON-EMPLOYEES. Employees shall 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 shall 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 shall immediately return all CCI in his or her possession. Employees shall 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") shall be limited to those with a need to access the information ("Authorized Users"). Senior Managers shall have the sole

authority and responsibility for determining and approving Authorized Users and their specific level of access to CCI.

The Corporate IT Department shall 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 shall arrange for electronic files containing trade secrets to be encrypted.

Access to CCI shall 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 shall prohibit an individual user from exceeding his or her authorized access.

When a new Employee reports for duty or there is a change in job responsibilities, his or her immediate supervisor shall 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 shall 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 shall send the approved request to the person in the Corporate or local IT Department charged with creating user accounts.

Systems users shall 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 shall secure their usernames and passwords to prevent unauthorized use, and shall properly log out of systems when they have completed use.

When any Employee leaves the Company, the local HR representative shall 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 shall 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.

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 shall be responsible for ensuring the appropriate level of security and access control measures for their facilities. Senior Managers and immediate supervisors shall also be responsible for determining the level of physical access required by each Employee. Senior Managers shall 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 to Company facilities shall be escorted and monitored while on the Company's premises.

Physical access to the hardware of computer systems containing CCI shall 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 shall be properly secured at all times in a locked office, drawer or safe. Such documents and electronic files shall not be left unattended in an accessible location at any time.

Where feasible, a system (e.g. a physical log or computer security program) shall 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 shall be properly deleted so as to be unrecoverable using ordinary means.

Annual Training
All Employees shall receive annual training on this Policy as part of Code of Conduct training.

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

Insider Trading

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.

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;
- 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.

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.

Event-Specific Blackout Periods

On occasion, certain officers, directors and/or other individuals may become aware of an event that is material to the Company that has not yet become public. 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, and/or other individuals 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 and Officers

Directors and officers of the Company, as well as any other individual making trades for the Company's account, are required to notify the General Counsel. The General Counsel (or, in the General Counsel's absence, the Chief Financial Officer of the Company) must pre-clear any trade **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 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.

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.

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.

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

Certain Company directors and officers have entered into Rule 10b5-1 trading plans approved by the Company's board of directors. Directors and officers who have entered into these plans need not adhere to the above requirements in this 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, and 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 shall 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 shall 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 shall 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 shall 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 shall 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 shall be less than $100 USD (per person), and the value of the meal or entertainment expense shall be less than $300 USD (per person), unless the Vice President, Administration 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 shall 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 Vice President, Administration 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 shall 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 shall 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 shall complete a due diligence questionnaire, and, where necessary, visit the third party's place of business. All due diligence efforts shall be documented, including any adverse information that is discovered. All adverse findings (including refusals to answer questions) shall be discussed with the Corporate Legal Department.

Each General Manager shall be responsible for transmitting all due diligence records in .pdf to the Corporate Legal Department. The Corporate Legal Department shall 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) shall 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 emails 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 Audit Departments shall include an anti-bribery compliance review as part of their due diligence of any proposed merger, acquisition, or joint venture. The review shall be in accordance with the principles outlined in this policy.

ANNUAL TRAINING

All directors, officers, and employees shall 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 shall have an additional annual training requirement concerning the specific requirements of their jobs. New hires shall receive training as part of their orientation.

ANNUAL CERTIFICATION

Each director, officer, and employee, shall 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) shall sign such acknowledgement and reaffirmation every three years after first signing such acknowledgement. Each President and General Manager shall cause these certifications to be sent to the Corporate Legal Department.

CONTACT REPORT REQUIREMENT

All Sensient directors, officers, and employees shall 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 shall 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 shall apply in all respects. No employee will be penalized for making a report in good faith.

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

AUDITS

As part of its regular audit duties, the Audit Department shall conduct a regular review of corporate books and records to ensure compliance with this policy. The Corporate Legal Department shall assist the 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 Audit Department shall 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 Audit Department shall conduct a review of all other third parties that interface with foreign officials no less than every 24 months. The Audit Department may retain local audit firms to assist in this process as necessary.

ANTI-BRIBERY COMPLIANCE OFFICER

The General Counsel shall 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 shall also issue periodic updates to all employees regarding anti-bribery and anti-corruption issues.

The Anti-Bribery Compliance Officer shall 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 shall be submitted to the Audit Committee of the Board of Directors for approval.

QUARTERLY REPORTS TO THE AUDIT COMMITTEE

The Anti-Bribery Compliance Officer shall 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 Audit Department, shall 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 shall 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 shall 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 shall 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 shall 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.

While working on behalf of Sensient, 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 shall 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 shall 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.

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

_____
Signature/Date

THE SENSIENT ANTI-BRIBERY POLICY:

Sensient shall 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, shall 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 shall be posted in a conspicuous location in every Sensient facility.

SAMPLE

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 of Conduct 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 division. 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 this 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:

Code of Conduct
GLOSSARY

Antitrust: Laws and regulations governing anticompetitive business conduct.
Audit: An official examination of accounts or records to see that they are in order.
Blacklist: A list of persons or organizations subject to punishment or unfavorable treatment.
Boycott: To refuse to have anything to do with; refuse to handle or purchase.
Circumvent: To evade, to find a way around.
Commodity: A product or exchange of trade.
Compliance: Action in accordance with a request or regulation.
Defamatory: Communication that attacks a reputation or speaks ill of.
Deleterious: Harmful to the body or mind.
Discriminatory: That which makes an unfair judgment or creates unfair treatment on the basis *of a prejudice or other unacceptable preconception.*
Disparagement: Communication that belittles or slights.
Due Diligence: The legal concept of a thorough review of facts, documents and records, usually in connection with a business transaction.
Elicit: To draw or bring out or forth.
Embargo: Any restriction placed upon commerce and business conduct by rule or order.
Explicit: Fully and clearly expressed or demonstrated, leaving nothing merely implied.
FCPA: "Foreign Corrupt Practices Act"
GRAS: "Generally Recognized As Safe"
Good Manufacturing Practices: Mandatory minimum manufacturing quality control procedures. Broad, general requirement applicable to Company food manufacturing facilities.
Indiscriminate: Not discriminating; lacking in selectivity on any basis.
Innuendo: An indirect message about a person or thing, generally of a negative nature.
Insider Trading: Illegal stock market activity that is done using material nonpublic knowledge gained through an association with any of the companies related to the stock or stocks transacted.
Material Inside Information: Information is MATERIAL if a reasonable investor would consider the information in making a decision to buy, hold or sell stock. Information is INSIDE if it is nonpublic; that is, not publicly announced and sufficiently communicated to the general public.
Monopolize: To create a situation by one group of exclusive control of producing or selling a service or commodity.
Nominal value: Small or trifling in amount. *The gift had only nominal value.*
Pertinent: Having logical, precise relevance to the matter at hand.
Proprietary: Rights which are exclusively owned by an individual or corporation, sometimes under a trademark or patent.
Protocol: A code of correct conduct and standard procedures.
Pursuant: In accordance with or as a consequence of. *Pursuant to the law, we are all sure to buckle our seatbelts while driving.*
Retribution: Something given or demanded in repayment.
Subsequent: Following in time or order; coming after.

Technical Data: Information of any kind that can be used or adapted to design, produce, manufacture, use or reconstruct articles or materials.

Tipping: The unlawful practice of communicating nonpublic information to outside parties who may use that information to purchase or sell stock in Sensient Technologies Corporation or related companies.

Token Value: Value that is symbolic rather than financial.

Tying: An agreement to sell a product only on the condition that the customer purchase another product.

Vest: To give the absolute right of ownership.

Window Period: The period of time in which Sensient Technologies Corporation directors and elected officers ordinarily can make transactions in Company stock. These periods coincide with the Company's announcement of quarterly and annual financial results (the four 30 calendar day periods that begin twenty-four hours after the Company's issuance of a press release announcing financial results for the prior fiscal quarter or fiscal year). The window period regulation was created to reduce the risk of inadvertent violation of insider trading